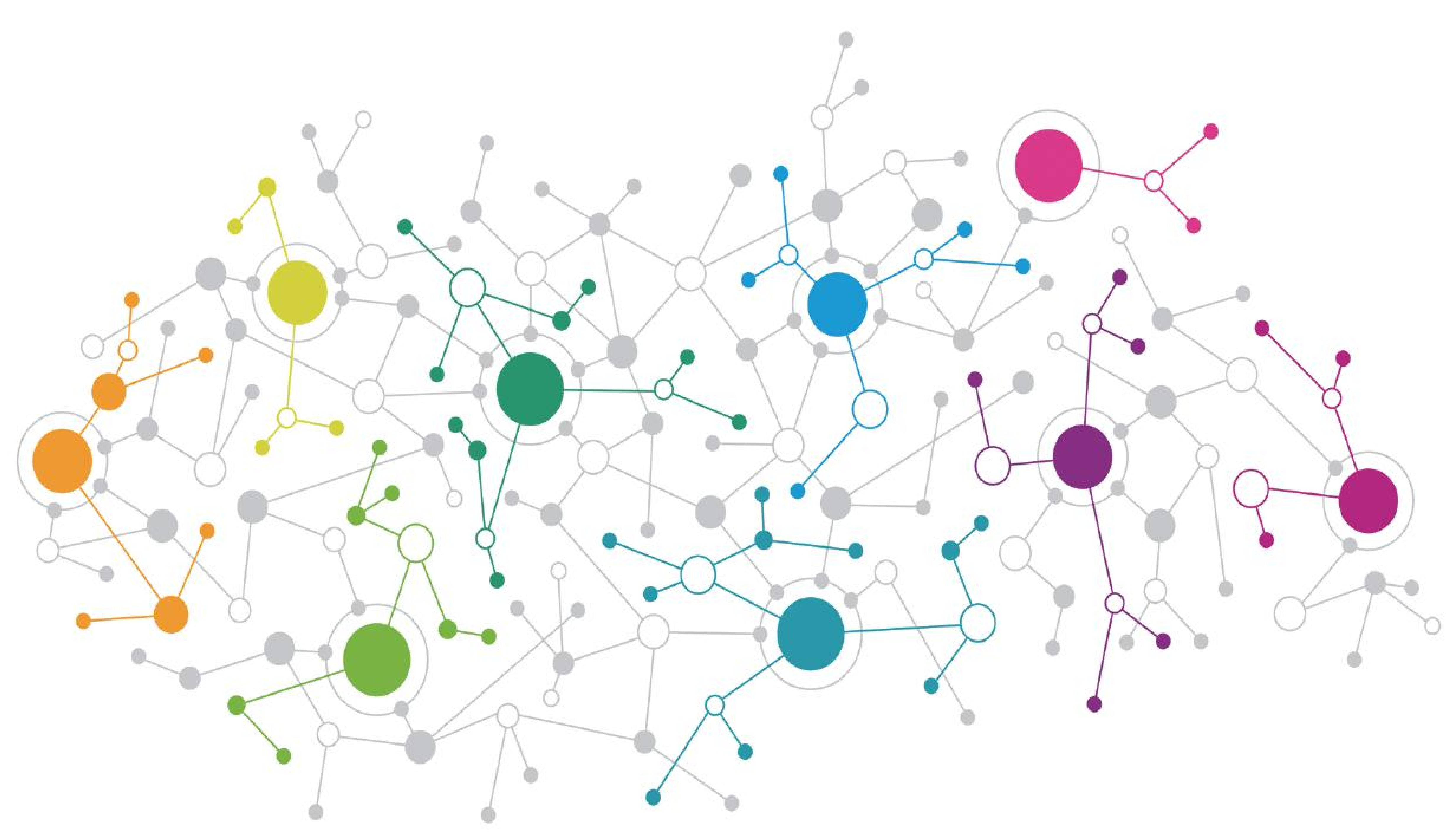


本书编著团队系华为公司在国内外区块链技术和应用领域的深度实践者。



区块链
技术及应用

华为区块链技术开发团队 编著

由浅入深地介绍技术缘起、原理、演进和发展趋势，

分享剖析实际落地案例并示范应用实践过程，探究区块链价值及未来发展趋势。

清华大学出版社

区块链技术及应用

华为区块链技术开发团队　编著

清华大学出版社
北　京

图书在版编目(CIP)数据

区块链技术及应用/华为区块链技术开发团队编著. —北京:清华大学出版社, 2019
ISBN 978-7-302-52383-3

Ⅰ. ①区…　Ⅱ. ①华…　Ⅲ. ①电子商务-支付方式-研究　Ⅳ. ①F713.361.3

中国版本图书馆 CIP 数据核字(2019)第 038779 号

责任编辑:王巧珍
封面设计:傅瑞学
责任校对:王凤芝
责任印制:杨　艳

出版发行:清华大学出版社
　网　　址:http://www.tup.com.cn, http://www.wqbook.com
　地　　址:北京清华大学学研大厦 A 座　**邮　编:**100084
　社 总 机:010-62770175　**邮　购:**010-62786544
　投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn
　质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn
印 装 者:北京嘉实印刷有限公司
经　　销:全国新华书店
开　　本:185mm×240mm　**印　张:**15.25　**字　数:**329 千字
版　　次:2019 年 3 月第 1 版　**印　次:**2019 年 3 月第 1 次印刷
定　　价:68.00 元

产品编号:082814-01

序　一
揭开区块链的神秘面纱

2009 年,区块链伴随着比特币系统诞生。经过比特币类加密数字货币的“疯狂”和区块链技术在诸如金融、供应链、政务等行业的应用,人们不断感受到这种新技术的魔力,同时区块链也成为技术创新的热词。区块链是当下最受人关注的方向之一,却又让人充满了雾里看花的感觉。可以说,区块链这个名词虽然已经被大家熟悉,但人们对于区块链到底是什么却又充满了疑惑。究其原因,一方面,区块链是一种新技术,处于发展初期,而且区块链技术、生态、工具和应用正在快速发展和演进,每个人的关注点不同,导致一千个人心中有一千个“哈姆雷特”;另一方面,区块链宣传推广的不同主体,出于商业或理念的差异,从各自的角度宣扬区块链应用和所带来的价值,不同行业的从业者从不同的维度仅看到区块链的“冰山一角”,甚至很多人对区块链的理解仅止步于比特币类加密数字货币。

每个人对区块链可能都有着不同的理解,我们可以从两方面来看待这种情况:一方面,区块链技术从业者正尽力让每个人的理解趋于一致;另一方面,存在不同的理解很正常,也很有益,因为这种多样化的观点碰撞恰恰是创新灵感的源泉。但一个不争的共识就是,区块链正在从理论的探索,逐渐走向落地,并快速发展壮大。区块链作为一种新技术,具备透明可信、防篡改、可追溯、去中心化/多中心等各种应用都十分需要的特性,应用已由金融领域延伸到供应链管理、政务服务、能源、版权存证、物联网等多个领域,满足了相互不信任的多个参与者建立分布式信任的需求,实现了低成本、高效的多方协同。随着区块链从金融领域向其他各领域的渗透,区块链技术逐步步入“区块链 +”的时代,可以预见“区块链 +”将像“互联网 +”一样为各行业注入新的活力。未来,随着各种应用对“可信”要求的增强,区块链的这些特性逐步成为各应用系统的“标配”,区块链技术也将逐步渗透到诸如操作系统、数据库、云平台等基础软件中。

区块链技术正在快速发展,在过去 10 年间已经历了以加密数字货币为标志的“区块链 1.0”和以智能合约为标志的“区块链 2.0”,目前进入了建立跨组织互信的“区块链 3.0”应用阶段,

与各种技术的结合正在加速,在各传统行业的产业价值也逐渐凸显。比如,区块链与云计算结合提供区块链云服务,极大降低了区块链的部署成本和技术门槛,让政府、企业等用户能够快速上手区块链,并通过实际落地应用感受区块链带来的价值。

近年来各国政府机构、国际货币基金组织以及标准、开源组织和产业联盟等纷纷投入区块链产业技术推动、标准拉通和应用落地推进的大潮中。随着区块链的产业价值逐渐明晰确定,区块链迅速引发了一场全球参与竞逐的“军备”大赛。同时从技术发展来看,区块链与人工智能、量子信息、移动通信、物联网等技术正在成为新一代信息技术的基石,其构建的可信机制,将有可能改变当前社会的商业模式,从而引发新一轮的技术创新和产业变革。

那么,区块链到底是什么?有什么价值?它对我们有什么影响以及如何使用这种新技术?它的未来将走向何方?这些都是值得我们思考的问题。在此之际,很欣喜能看到这样一本系统讲解区块链技术、应用场景和未来发展前景的图书出版。作者来自华为区块链技术开发团队,有丰富的技术创新和应用推广经验。本书从区块链诞生与发展的角度开篇,然后介绍了区块链的核心技术,接下来通过实际案例阐述了区块链如何与各行业相结合解决痛点问题,最后进一步展望了区块链的未来发展趋势。希望广大读者通过阅读此书,能够很好地了解区块链的本质,理解其更深层次的内在逻辑,感受区块链技术在经济与社会等各个领域的显著作用和重要影响。

区块链作为一项新技术,虽然在应用方面暂时面临一些尚待解决的问题与挑战,但这也是新技术发展过程中的正常情况。恰恰是因为这些问题与挑战的存在,才促进了技术的不断发展与成熟。另外,区块链的落地,不只是技术问题,还涉及法律、经济等多方面的因素,需要各界仁人志士共同推动,给予区块链技术更多的包容与关爱,让区块链这项新技术有更多成长的沃土与空间,使它能够孕育出更美丽的花朵。对于区块链的未来,我们充满期待。

“长风破浪会有时,直挂云帆济沧海”,相信区块链在未来能够更好地将“可信”数字世界带入每个人、每个家庭、每个组织,构建万物互联的“可信”智能世界。

华为云 BU CTO
张宇昕

序　二

用发展的眼光看待区块链技术

互联网技术的出现极大加快了信息传递的速度,降低了人类社会的信息传递成本,也深刻地改变了人们的生产方式、生活方式,并已经渗透到方方面面。当前互联网只是信息传递者,即为信息互联网,它并不关心人与人之间的协作模式和信任构建方法。而区块链在信息互联网的基础上构建了一种新的可信的大规模协作方式,以解决数字经济发展的信任问题,被誉为下一代互联网的重要特征,因此区块链被寄予众多期望。李克强总理在写给 2017 中国国际大数据产业博览会的贺信中表示:“当前新一轮科技革命和产业变革席卷全球,大数据、云计算、物联网、人工智能、区块链等新技术不断涌现,数字经济正深刻地改变着人类的生产和生活方式,作为经济增长新动能的作用日益凸显。”

2008 年底,一个化名中本聪的神秘人士(也可能是一个组织)在网络上发表了后来被称为“比特币白皮书”的论文,两个月后发布并开源了比特币系统,区块链的序幕就此拉开。近十年间涌现出数千种加密数字货币,也催生出不计其数的 ICO 案例。当然,最值得人们关注的还是区块链技术的发展演进。它脱胎于比特币,但却以一种独立的姿态茁壮成长。区块链作为哈希算法、数字签名、点对点传输、共识机制等多种已有技术的集成组合创新,具有抗抵赖、防篡改、可追溯、安全可信等“神奇”特性,“巧妙”地解决了多方可信协同问题,正在广泛应用于金融、供应链、政务等领域。用数据库做个对比,以数据库为核心的信息系统解决了组织内的信息管理问题,以区块链为核心的信息系统实现了组织间的可信数据管理、共享及高效协作,是对当前信息系统的有效补充。

区块链技术经常被冠以“颠覆性”技术的名号,这种名号为区块链技术的发展带来了备受关注的光环,促进了区块链技术的发展,也同时带来了一定的压力、误解甚至质疑。当前区块链技术正处于初级且快速发展阶段,回首云计算的发展历程,2010 年云计算的概念和当前被大家广为接受的云计算概念已经极大不同。我们不可能直接跳到最终理想的终点,发展过程中应用驱动的中间态技术积累演进必不可少,需要业界仁人志士的共同努力,积极踏实地投

入区块链基础技术研究及服务实体经济的应用推进中。另外,区块链应用的推进较普通应用难度大,尤其是因为区块链应用涉及多个参与方,原本单个组织要构建一个信息系统就要经过内部激烈的讨论,多个参与方共同讨论构建一个新的协作机制和系统的难度可想而知。虽然推进难度不小,但是我们已经看到了很多成功的价值案例。越是颠覆性的东西推广起来阻力越大,而一旦迸发将势不可当。我们要用发展的眼光看待区块链技术,坚信基于区块链技术所构建的新的协作方式能够助力实体经济往更深层次发展。

我很高兴看到本书是基于华为公司在区块链技术应用实践方面的经验,从用户的视角,用通俗的语言介绍了区块链技术的基本原理、服务实体经济的应用场景,并以华为公有云区块链服务 BCS 为例做了翔实介绍,其中部分场景已经获得商用并取得良好收益。希望读者能够通过本书客观地理解区块链技术的价值,深入了解区块链技术本质以及区块链如何巧妙地与应用场景相结合。

用发展的眼光看待区块链技术及应用,未来已来,将至已至。

用战略的眼光看待区块链技术及应用,以变革的姿态迎接未来,决胜未来。

华为 Fellow①

胡子昂

---

① Fellow:代表华为公司专业技术人员重大成就的最高称号。

前　言

以比特币为代表的加密数字货币是区块链的应用之一。区块链不等于比特币，区块链作为一种革新的技术，已经被应用于许多领域，包括金融、政务服务、供应链、版权和专利、能源、物联网等。未来，与区块链技术接触的群体将会越来越多，对区块链技术进行更加深入的了解与探究将是很多领域的创新创业中不可或缺的一环。

区块链技术现已孕育出了大量的创业公司，而同时许多大公司也展开了对区块链技术的探究与布局。华为公司作为高新科技的领军者之一，对区块链技术已经投入了大量的研究，拥有了丰富的实践经验。我们创作本书的目的，一方面，当前提到区块链，有人会将其与比特币或各类加密数字货币画等号，我们希望借助本书消除读者的这种误解，使读者能够明白比特币或各类加密数字货币只是区块链的一种应用；另一方面，我们希望将长期以来在区块链技术的知识积累，以及对区块链在各领域应用的实践和思考，分享给广大的读者。我们希望不了解区块链的读者能够通过本书对区块链有一个系统而详尽的认识，而对区块链有所了解的读者能够通过本书获得新的启发与感悟。

关于本书

本书的目标读者是所有想充分了解区块链技术和应用的人。本书既包含区块链的基础知识，又有对区块链的应用场景以及发展趋势的探究，可以帮助非专业开发人员对区块链做系统了解。同时，本书也有对一些技术细节和算法的讨论，并以华为云区块链服务为示范平台介绍了区块链应用实践的过程，期望帮助区块链开发人员更加快速、深入地投入区块链的开发工作当中。

华为区块链技术开发团队是由教授、博士、留学归国人员、华为海外研究所科研人员和技术骨干等组成的一支高水平技术研究团队，在区块链相关的领域，如分布式系统、算法、密码

学、网络、数据管理等,都有丰富经验,平均从事相关业务经验超过6年;成功推动了多个政务、金融、供应链、存证等应用落地,担任可信区块链推进计划BaaS组组长,积极参加中国计算机学会CCF区块链专业委员会、ITU-T等行业、学术和标准组织。本书是由曹朝博士主持的华为区块链技术开发团队合作完成的,作者包括(排名不分先后):曹朝、蔡春瑜、陈黎君、丁健、郭凯、韩士泽、黄东润、金钊、雷宇宁、李保松、李继忠、厉丹阳、刘奇、刘勋、刘元章、刘再耀、罗玉龙、马新建、潘义峰、檀景辉、姚序明、王磊、张秦涛、张小军、张煜、张子怡、周萌萌。

本书的内容

本书系统详实地讲解了区块链技术的各个方面,主体内容包括三大部分:区块链演进及技术介绍、区块链的应用、区块链未来的价值和发展趋势探究。

本书对区块链基础知识的介绍从区块链的鼻祖——比特币开始,然后介绍区块链的技术基础,比如共识算法和智能合约,并由此说明它的特性,比如透明性和不可篡改性。本书还通过介绍区块链的发展历程以及区块链的不同类型,使读者对区块链整体有基本了解。

介绍完基础知识以后,本书对区块链的价值和应用场景做了进一步的讨论,主要分析了金融、供应链、政务服务、存证与版权、能源五大行业的业务场景、现状及痛点、区块链解决方案和价值。最后总结了判断某个领域能否应用区块链技术的五个准则,这部分内容对于创业创新和投资决策都有一定的借鉴意义。书中还以华为云区块链服务为例,展示了如何使用区块链服务快速开发区块链应用,为感兴趣的开发人员提供参考。

本书还收集了业界对于区块链的不同观点,以及关于区块链的一些常见问题,并对几个常见的区块链平台做了简单的介绍,同时对区块链未来可能的应用领域、产生的价值及发展趋势进行了展望。

本书虽然系统地从各个方面阐述了区块链的各种知识,但各个章节之间相对独立,便于读者查阅参考。对某些章节已经比较了解的读者,可以直接跳到感兴趣的章节进行阅读。我们相信本书能够使读者以一种最有效率的方式充分地了解区块链。

勘误和支持

由于编写时间仓促,编写人员水平有限,书中内容出现疏漏在所难免。如果读者发现任何问题和不足,还请不吝指正。如果对本书内容有任何的疑问,也欢迎通过出版社联系我们。我们将十分感谢读者的反馈,并会及时对本书内容作出勘误和修改。

致谢

本书是由华为区块链技术开发团队完成的,大家在繁忙的开发工作中抽出时间编写书

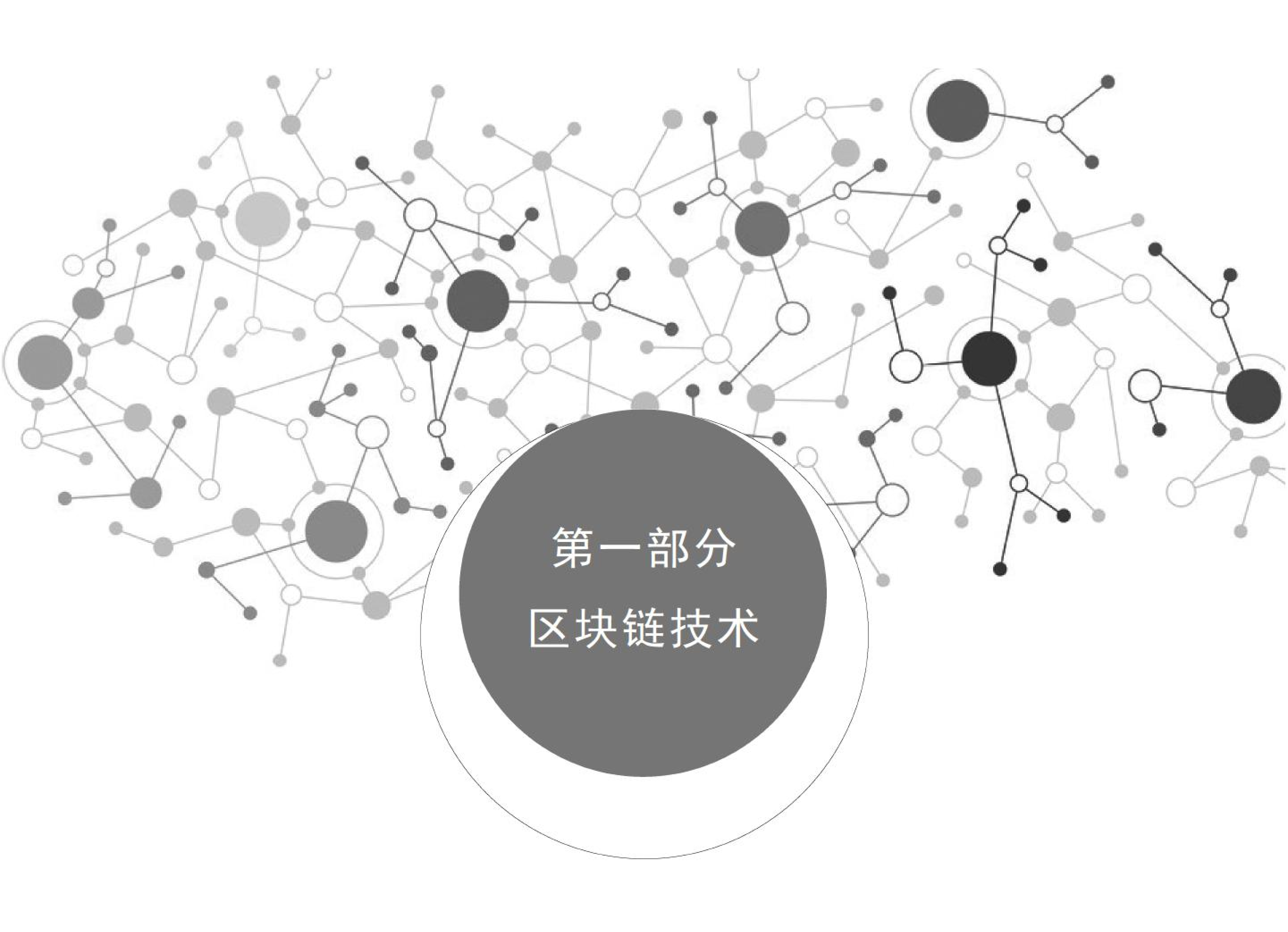
稿，感谢大家的辛苦付出，同时感谢徐直军、李英涛、郑叶来、龚体、胡子昂、廖振钦、杜娟、黄津、金雪锋、杨开封、樊薇萱、万汉阳、陈威、饶争光、俞岳、郑文钦和宋承朝，以及华为公司其他主管对我们写作的大力支持。感谢邢紫月与出版社的大量沟通，促成了本书的快速出版。还要感谢雷宇宁和韩士泽承担了全书的审阅工作，给出大量有价值的建议。最后，感谢我们每一位家人的支持陪伴，我们的工作因为有了家人的支持和期待才变得更有意义。

华为区块链技术开发团队

2018 年 12 月

目　录

第三部分 区块链未来



第一部分
区块链技术

区块链技术来源于比特币,也因为比特币的疯狂而备受瞩目。区块链技术发展到现在,无论是在技术上的深度与广度,还是在应用场景上的宽度,均取得了较大突破。虽然比特币类加密数字货币在区块链领域依然备受关注,但是百花齐放的区块链应用,尤其是大量企业级区块链应用的出现正在催熟区块链技术,区块链技术正处于快速发展演化期,未来会拥有一个更大的可以施展拳脚的舞台。

第 1 章

疯狂的比特币及其原理机制

1.1 比特币的诞生

2008 年 11 月,一位化名为中本聪(Satoshi Nakamoto)的人,在密码学论坛 metzdowd. com 发表的一篇名为 *Bitcoin: A Peer-to-Peer Electronic Cash System*(《比特币:一种点对点的电子现金系统》)的论文中首先提出了比特币。2009 年 1 月 3 日,中本聪发布了比特币系统并挖掘出第一个区块,被称为“创世区块”,最初的 50 个比特币宣告问世。同时有趣的是,中本聪在创世区块中带上了一句话以证明这个区块挖出于 2009 年 1 月 3 日,这句话就是图 1. 1 中的《泰晤士报》2009 年 1 月 3 日的头版新闻标题——*Chancellor on brink of second bailout for banks*(《财政大臣正处于第二次救助银行之际》)。图 1. 2 是创世区块的原始二进制数据及其 ASCII 码文本表示,可以看到其中所携带的标题信息,在图中已用方框圈出。

截至 2018 年,比特币系统已经运行了整整十年。比特币系统软件全部开源,系统本身分布在全球各地,无中央管理服务器,无任何负责的主体,无外部信用背书。在比特币运行期间,有大量黑客无数次尝试攻克比特币系统,然而神奇的是,这样一个“三无”系统,近十年来一直都在稳定运行,没有发生过重大事故。这一点无疑展示了比特币系统背后技术的完备性和可靠性。近年来,随着比特币的风靡全球,越来越多的人对其背后的区块链技术进行探索和发展,希望将这样一个去中心化的稳定系统应用到各类企业应用之中。在本书第二部分,我们将选取代表性行业为例,讲述比特币背后区块链技术的各类相关应用。



THE TIMES

Saturday January 3 2009 timesonline.co.uk No 69523

£1.50

Eat Out from £5

More than 900 great restaurants, including four **Gordon Ramsay** favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Michael Sheen Frost, Nixon and me

Magazine

Working mums So that's how she does it

Detox in style The best spas on the planet

Travel

Salmon Rushdie I Won't Marry Again

Giant Killing? Guide to the FA Cup Third Round

Sport

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

99p

Continued on page 6, col 1

Leading article, page 2

图 1.1 《泰晤士报》2009 年 1 月 3 日的头版

图片来源：https://dollarvigilante.com/blog/tag/satoshi-birthda

```
00000000  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E  ....;£íýz{.²zÇ,>
00000030  67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA  gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040  4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C  K.^J)«_Iÿÿ...¬+|
00000050  01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00  ................
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00000070  00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D  ......ÿÿÿÿM.ÿÿ..
00000080  01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F  ..EThe Times 03/
00000090  4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C  Jan/2009 Chancel
000000A0  6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20  lor on brink of 
000000B0  73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66  second bailout f
000000C0  6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05  or banksÿÿÿÿ..ò.
000000D0  2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27  *....CA.gŠý°þUH'
000000E0  19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6  .gñ¦q0·.\Ö¨(à9.¦
000000F0  79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4  ybàê.aÞ¶Iö¼?Lï8Ä
00000100  F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57  óU.å.Á.Þ\8M÷º..W
00000110  8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00           ŠLp+kñ._¬....
```

图 1.2 创世区块原始数据

资料来源：https://en.bitcoin.it/wiki/Genesis_block

除了其背后的技术所具有的价值，比特币作为一种虚拟货币，也逐渐与现实世界的法币建立起了“兑换”关系，其本身有了狭义的“价格”。现实世界中第一笔比特币交易发生在

2010 年 5 月 22 日,美国佛罗里达州程序设计员拉斯洛·豪涅茨(Laszlo Hanyecz)用 1 万个比特币,换回了比萨零售店棒约翰(Papa Johns)的一个价值 25 美元的比萨。这是比特币作为加密数字货币首次在现实世界的应用。按照这笔交易,一个比特币在当时的价值为 0.25 美分。然而在今天来看,1 万个比特币可以说是一笔巨款(注:按照 2018 年 9 月的价格计算,1 万个比特币大约值 6 000 多万美元),但在比特币刚出现时,人们并没有意识到这种新生事物在未来将会引起的疯狂及宏大的技术变革。

1.2　疯狂的比特币

1.2.1　疯狂的比特币价格

比特币自诞生之日起,经历了多次的暴涨暴跌,其价格的变动犹如过山车一般。

在 2011 年 1 月,1 个比特币还不值 30 美分,但在随后的几个月里,它的价格一路走高,突破了 1 美元,很快上升到 8 美元,然后是 20 美元。到 2011 年 6 月 9 日,1 个比特币的价格已经涨到了 29.55 美元,半年时间涨幅约为 100 倍。但是随后不久,比特币交易平台 Mt. Gox 由于其交易平台本身的漏洞被黑客攻击,使平台本身和其用户蒙受了较大的损失,比特币的安全性受到了投资者们的质疑。因为该事件,比特币价格持续走低,急剧回落,在仅仅半年时间后的 2011 年 11 月,比特币的价格已经低至 2 美元,相比 6 月份的最高价跌去了 90% 以上。

2012 年 12 月 6 日,世界首家比特币交易所在法国诞生,比特币单价重回巅峰期,单枚涨至 13.69 美元。2013 年 3 月,按照当时的兑换汇率,全球发行比特币总值超过 10 亿美元,这也是比特币价格飞涨的一年。在同年 12 月,单枚比特币的价格突破 1147 美元,超越了当时的国际黄金价格。

2014 年到 2016 年,比特币市场持续低迷。2015 年 8 月,比特币单枚价格跌至 200 美元;随后的 2016 年,比特币市场迎来内外环境的巨大变化和影响:内部变化是根据比特币的既定规则,其年产量开始收缩,意味着比特币收获难度增高;外部影响则源自英国脱欧、美国大选、亚洲投资者激增等事件。在内外因素的共同作用下,比特币的价格持续上涨,截至 2016 年 12 月,单枚价格又一次突破了 1 000 美元。

2017 年是比特币发展史上十分重要的一年,全年整体涨幅高达 1 700%。2017 年一整年,比特币价格走势图犹如一轮过山车,暴增暴跌让投资者为之疯狂。在 2017 年全年,比特币最低价格是 789 美元,对应日期为 1 月 11 日;最高价位为 19 142 美元,对应日期是 12 月 18 日。其中,1 月到 5 月比特币价格缓慢增长,到 5 月中旬达到 2 000 多美元/枚,但进入六、七月后又开始极速下跌,跌幅达到 45%。比特币价格的剧烈变动引起了各国政府的密切关注,同年 9 月,我国发布《关于防范代币发行融资风险的公告》,国内市场热度渐渐消退,但在全球市场上,日本和韩国比特币投资者持续涌入,比特币价格一路高涨,12 月 18 日触及历史峰值。然而随后迅速开始暴跌,12 月 31 日封盘价跌破 11 000 美元。

比特币货币市场在2017年辉煌一时,但2018年市场表现并不理想。受多方政策影响,比特币价格开始大幅度下跌。2018年1月的第一个星期,比特币有过短暂的升值期,1月7日达到峰值16 448美元,但从1月8日开始暴跌,仅1月8日一天就跌了2 219美元,跌幅达15.6%,后续几天有涨有跌,但总体趋势仍是持续走低。截至笔者发稿前(2018年11月8日数据),比特币单枚价格为6 520美元左右,相比2017年12月峰值19 142美元确实有了较大幅度的下跌,未来,数字加密货币市场的大起大落还将继续上演。2013年4月以来比特币价格走势如图1.3所示,从中可以对比特币价格的疯狂变动略窥一斑。

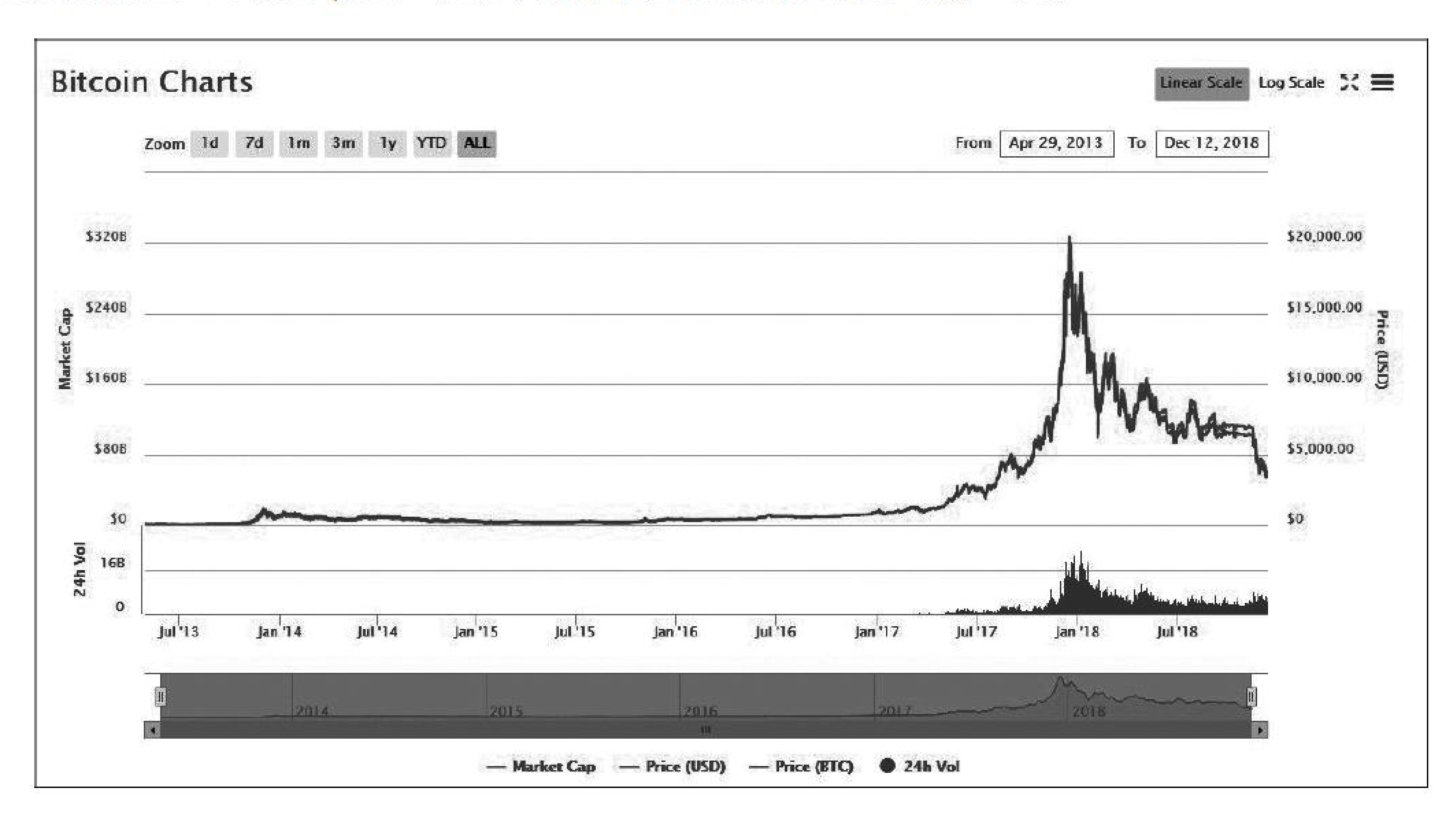


图1.3 从2013年4月29日至2018年12月12日比特币价格走势

资料来源:https://coinmarketcap.com/currencies/bitcoin/#charts

1.2.2 疯狂的矿机和芯片

在比特币疯狂的价格和犹如过山车般的价格波动吸引了越来越多投机者的同时,比特币矿机及芯片技术也取得了长足进展。所谓比特币“矿机”,就是用于赚取比特币的计算机。用户下载专用的比特币运算软件,在矿机上运行相应的软件,参与记账并获取对应的记账奖励。

比特币矿机的发展经历了三个阶段。第一阶段,即挖矿初期,挖矿的参与成本较低,只需要任意一台普通的计算机即可进行挖矿,同时,由于参与挖矿竞争的节点数目较少,挖矿算法的难度极低,用普通的CPU处理器就能达到不错的产出率,从而较容易获得比特币激励。第二阶段,挖矿中期,此阶段参与挖矿节点数目越来越多,普通CPU挖矿节点很难再获取较为可观的产出率。由于CPU的设计逻辑偏重浮点计算等通用计算需求,而比特币挖矿算法所涉及的仅为简单的哈希计算,不能够充分利用CPU的能力,一些矿工开始使用具有多处理器、能够进行快速的简单计算特性的显卡(即GPU)进行挖矿,相比于CPU挖矿,其运算效率和对应的

产出率都得到了大幅提升,此阶段即为矿机处理器由 CPU 向 GPU 的转变。第三阶段,参与挖矿的节点及其对应的算力进一步上升,进入了专业矿机的阶段。前两个阶段的通用计算机已不能满足矿工们的需求,因此出现了专门为比特币挖矿而设计的定制化机器,这类机器专门为哈希运算设计,能够更快地进行比特币挖矿过程所需的哈希运算。图 1.4 是一个市场上较为主流的矿机,该矿机的额定算力已经达到了 27TH/s,也就是每秒能够进行 2.7×10^{10} 次哈希运算。



图 1.4　比特币矿机示例

图片来源: https://m.bitmain.com.cn/product/detail?pid=00020181211094757815UgH3FPX20655

相应地,挖矿芯片的发展经历了从 CPU、GPU、FPGA 到 ASIC 的四个阶段,从通用型逐渐转向了挖矿专用型。其中,专用集成电路(Application Specific Integrated Circuits,ASIC)是指应特定用户要求或特定电子系统的需要而设计、制造的集成电路,本书是指为比特币挖矿专门设计的专用集成电路。ASIC 矿机芯片的制造流程先进、产品更迭速度极快。目前市场上主流的 ASIC 矿机芯片制造工艺从 110nm、55nm、28nm,一直升级到 16nm。2018 年,矿机厂商宣布推出 7nm 矿机,意味着矿机进入 7nm 时代。

在比特币矿机算力不断提升的同时,其进行挖矿消耗的总电量也是惊人的。英国《卫报》2017 年的一篇研究表示,比特币挖矿一年消耗的电力已经超过了 19 个欧洲国家一年所消耗的电力总和,包括克罗地亚、爱尔兰、冰岛、斯洛文尼亚以及拉脱维亚等。从全球范围来看,比特币一年的耗电量是全球耗电量的 0.13%。

需要说明的是,比特币巨大的耗电量主要源于其计算密集型的挖矿算法以及其所采用的工作量证明形式的共识协议。实际上,目前的众多面向企业级应用的区块链平台及应用通过根据其应用场景及环境采用不同的共识协议及相关算法,避免了不必要的能源消耗,使能源消耗与普通信息系统相当。

1.2.3　疯狂的矿场与矿池

随着比特币价格的震荡式飙升,人们仿佛像美国西部刚刚发现金矿一样,纷纷投入"挖矿"的事业之中。由于比特币的产生速率基本保持稳定,但对于单个节点来说,其挖到某个比特币的概率与其算力占所有参与挖矿竞争节点总算力的比例成正比,因此,随着参与到比特币挖矿竞争中的机器及算力大幅上升,单个节点或少量的算力能够成功挖到比特币的概率急剧下降,小规模挖矿参与者的收益难以得到保障,因此两种不同的组织相继登场,分别是矿场和矿池,它们的目的都是集中算力,提升挖矿概率,从而提升收益。

矿场是将挖矿产业化的产物。简单来说,矿场即为挖矿设备管理场所。早期的矿场非常简单,只有一些简单的机架供矿机的安置,同时仅提供简单的网络、电力等资源。随着专业挖

矿设备的不断增多,人们发现这种粗犷的管理方式下,设备太容易损坏,同时设备维修更新成本也很高。因此,通风防尘、温度湿度控制等数据中心管理常见的规范管理措施逐渐被运用到矿场中。由于矿场的电力消耗非常惊人,且噪音巨大,当前矿场一般选择建在人烟稀少且电力便宜的地区。当前矿场的管理模式完全向大型数据中心的管理靠齐,甚至很多大型矿场的规模已经不输很多大型数据中心。图 1.5 和 1.6 分别对某大型矿场外观和内部进行了展示。



图 1.5　矿场外观

图片来源: http://tech.163.com



图 1.6　矿场内部

图片来源: http://tech.163.com

除了矿场这种产业化的挖矿方式,还有一种将大量算力较低设备进行联合、共同运作挖矿的平台,即“矿池(Mining Pool)”,加入“矿池”的设备即被称作“矿工”。在“矿池”中,不论“矿工”所能提供的运算力的多寡,只要是通过加入矿池来参与挖矿活动,无论是否成功挖掘出有效区块,在该矿池挖矿成功后皆可经由对矿池的贡献(即投入的算力)来获得比特币奖励。亦即多人合作挖矿,获得的比特币奖励也由多人依照贡献度分享。这种组织方式实际上并没有提高单个矿工挖矿收益的期望值,但提升了单个矿工收益的稳定性。

截至 2018 年 10 月,根据 BTC.com 的分析,如图 1.7 所示,排名前六的比特币矿池占据整体比特币挖矿算力 61.4% 的份额,分别是 BTC.com(占比 17.4%)、蚂蚁矿池(antpool,15.3%)、ViaBTC(12.6%)、SlushPool(11.9%)、BTC.TOP(10.6%)、F2Pool(9.6%)。世界上最大的比特币矿池是蚂蚁矿池,算力达到惊人的 2 500PH/s,如果将超级计算机“天河二号”每秒 33P FLOPS(Peta FLOPS)的计算能力换算成哈希计算的话,大约是蚂蚁矿池的千分之一,单纯从哈希运算的角度来看,比特币矿池有超强的运算能力(注:比特币挖矿中需要做大量的哈希运算,因此矿机/矿池的算力就以每秒能执行的哈希运算次数来衡量。1kH/s 是每秒 1 000 次哈希;1MH/s 是每秒 1 000 000 次哈希;1GH/s 是每秒 10 亿次哈希;1TH/s 是每秒 1 000 000 000 000 次哈希;1PH/s 是每秒 1 000 000 000 000 000 次哈希)。

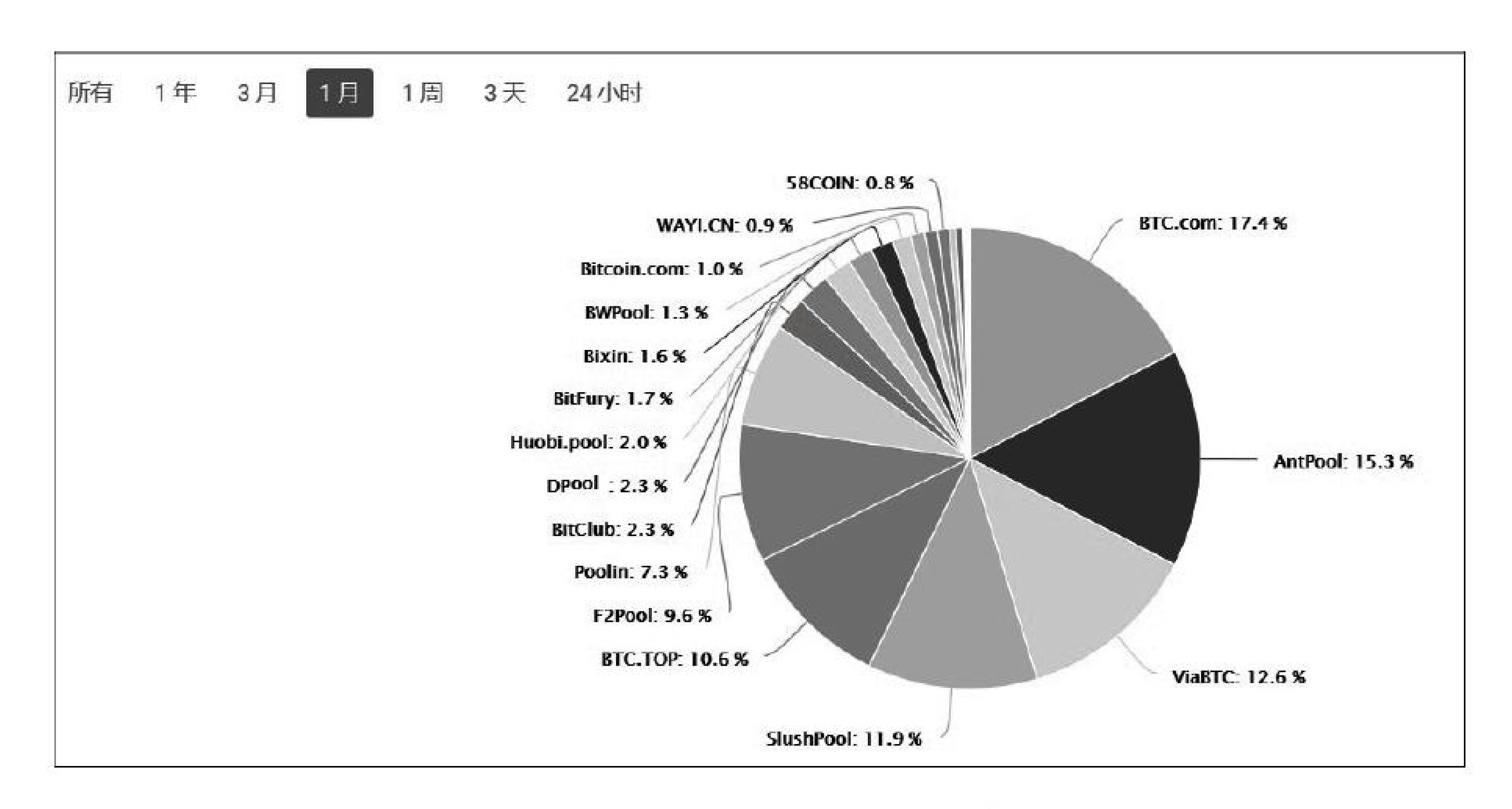


图1.7　截至2018年10月的矿池分布饼状图

资料来源：BTC. com

在2012年，矿池总算力之和已经接近比特币总算力的一半。近几年，矿池更是逐渐成为算力的主力，算力呈现集中化趋势。然而，这种集中化的趋势会带来一些弊端。由于在比特币世界中，算力高即代表着产生记账区块的概率高，即代表着“记账权”更强。如果矿池算力不断提升，单家矿池算力达到50%以上，即可以对比特币进行51%攻击，对比特币系统的开采权和记账权进行垄断。

1.3　比特币的通俗故事

那么什么是比特币呢？它背后到底有着什么神奇的地方，让如此多的人追捧，甚至是不惜消耗巨大的资源来获取它呢？让我们从一个通俗的故事开始，如图1.8所示。

从前，有个古老的村落，里面住着一群古老的村民，这个村庄没有银行为大家存钱、记账。没有一个让所有村民都信赖的村长来维护和记录村民之间的账务往来，也就是没有任何中间机构或个人来记账。于是，村民想出一个不需要中间机构或个人，而是大家一起记账的方法。

比如，张三要给李四1 000块钱。张三在村里大吼一声：“大家注意了，我张三给李四转了1 000块钱。”附近的村民听到了之后做两件事：(1)通过声音判断这是张三喊的，而不是别人冒名张三喊的，从而防止别人去花张三的钱；(2)检查张三是否有足够的钱，每个村民都有个小账本记录了各个村民有多少钱，当确认张三真的有1 000块钱后，每个村民都会在自己的小账本记录：“××××年×月×日，张三转给李四1 000块钱。”除此之外，这些村民口口相传，把张三转账的事情告诉了十里八村，当所有人都知道转账的事情后，大家就能够共同证明“张三转给李四1 000块钱”。这样，一个不需要村长(中心节点)却能让所有村民都能达成一致的记账系统诞生了。这个记账系统就可以类比为我们今天常说的比特币系统。

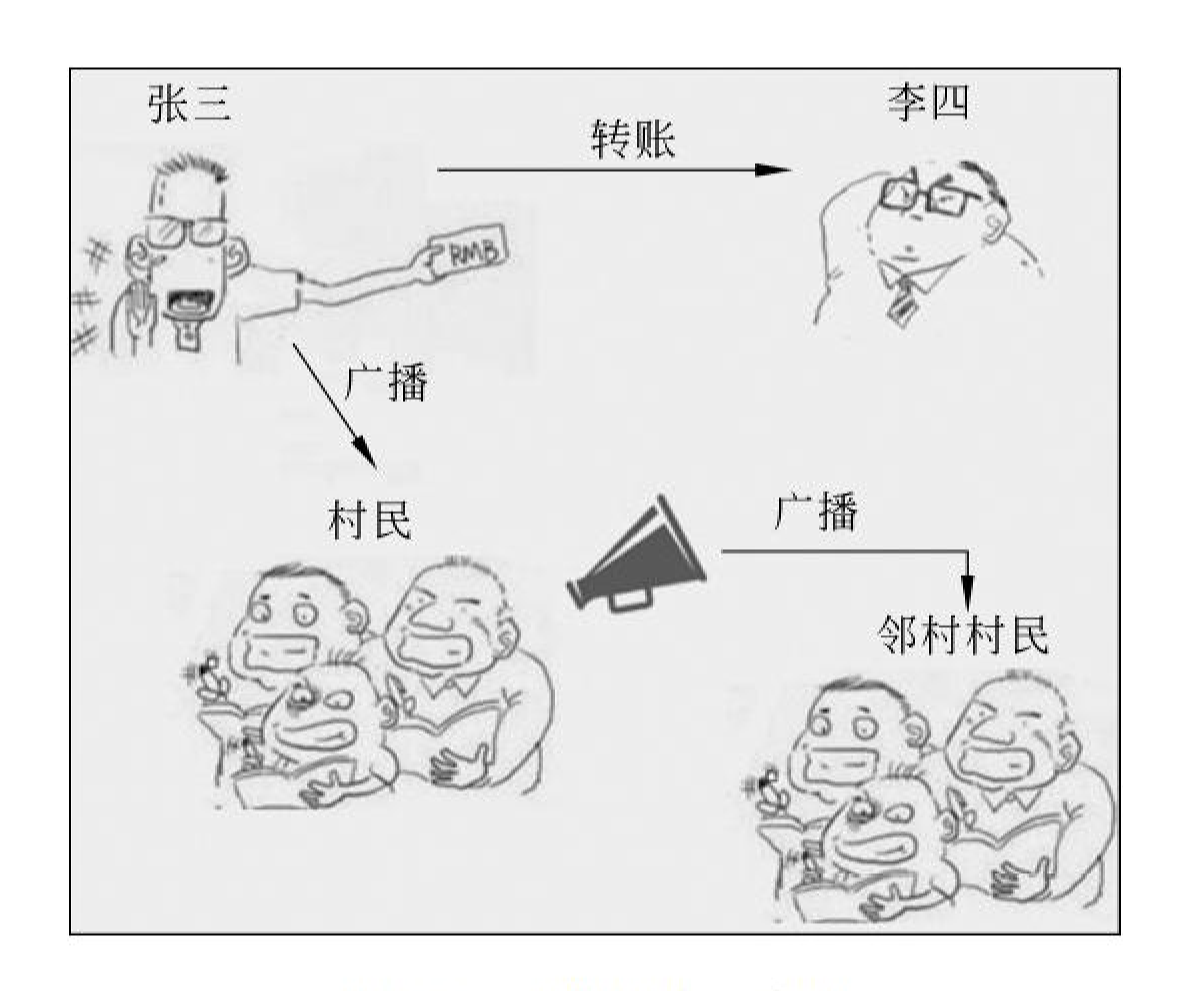


图 1.8　通俗故事示意图

资料来源：https://www.gingkoo.com/nd.jsp?id=12

故事到此并未结束，由此引出了三个值得思考的问题。

(1) 记的账在后面会不会被篡改？

(2) 村民有什么动力帮别人记账？

(3) 这么多人记账，万一记的不一致岂不是坏了，以谁记的为准？

比特币系统巧妙地解决了这三个问题。

第一，比特币采用两种策略保证账本不可篡改：①人人记账。人人手上都维护一本账本，这样即使某个人改了自己的账本，他也无权修改其他村民手上的账本，修改自己的账本相当于“掩耳盗铃”，别人是不会认可的。②采用“区块+链”的特殊账本结构。在这种账本结构中，每一个区块保存着某段时间内所发生的交易，这些区块通过链式结构连接在一起，形成了一个记录全部交易的完整账本。如果对区块内容进行了修改就会破坏整个区块链的链式结构，导致链条断了，从而很容易被检测到，这两个策略保证了从全局来看整个账本是不可篡改的。

第二，前面一条中提到了人人参与记账，大家肯定会问“凭啥要我帮别人记账呢”。这就涉及比特币系统中的激励机制。参与记账的村民，被称为“矿工”。这些矿工中，首个记账被认可的人：①将获得一笔奖励，这笔奖励就是若干个比特币，这也是比特币发行的唯一来源，这种奖励措施使众多矿工积极参加记账；②谁在某一块账本被认可，其他人都会分别拷贝这一块账本，从而保证所有人维护的账本是完全一致的。这两点保证了区块链的自动安全运行。

第三，既然有了激励，大家就会争抢着记账并努力让自己的记账被认可，怎么确定以谁记的为准呢？为了能够确定以谁记的账为准，村民们想到了一个公平的办法：对每一块账本（类比为我们现实账本上的一页），他们从题库中找了一道难题，让所有参与记账的“矿工”都

去破解这道难题,谁若最先破解了,该页/块就以他记的账为准。这个破解难题的过程,就被称为“挖矿”,也即工作量证明的过程。这里需要说明的是,这个难题的解题过程需要不断地尝试,较为困难,但是找到答案发给别人后,别人是很容易验证的。

因此,比特币通过“区块 + 链”的分布式账本保障了交易的不可篡改,通过发放比特币的激励措施激励了“矿工”的参与,通过计算难题(矿工挖矿)解决了记账一致性的问题。这样,完美地形成了一个不依赖任何中间人即可完成记账的自动运行系统。如图 1.9 所示,这其中具有“区块 + 链”不可篡改账本、多方参与、结果共识的技术,就是比特币背后的区块链技术。

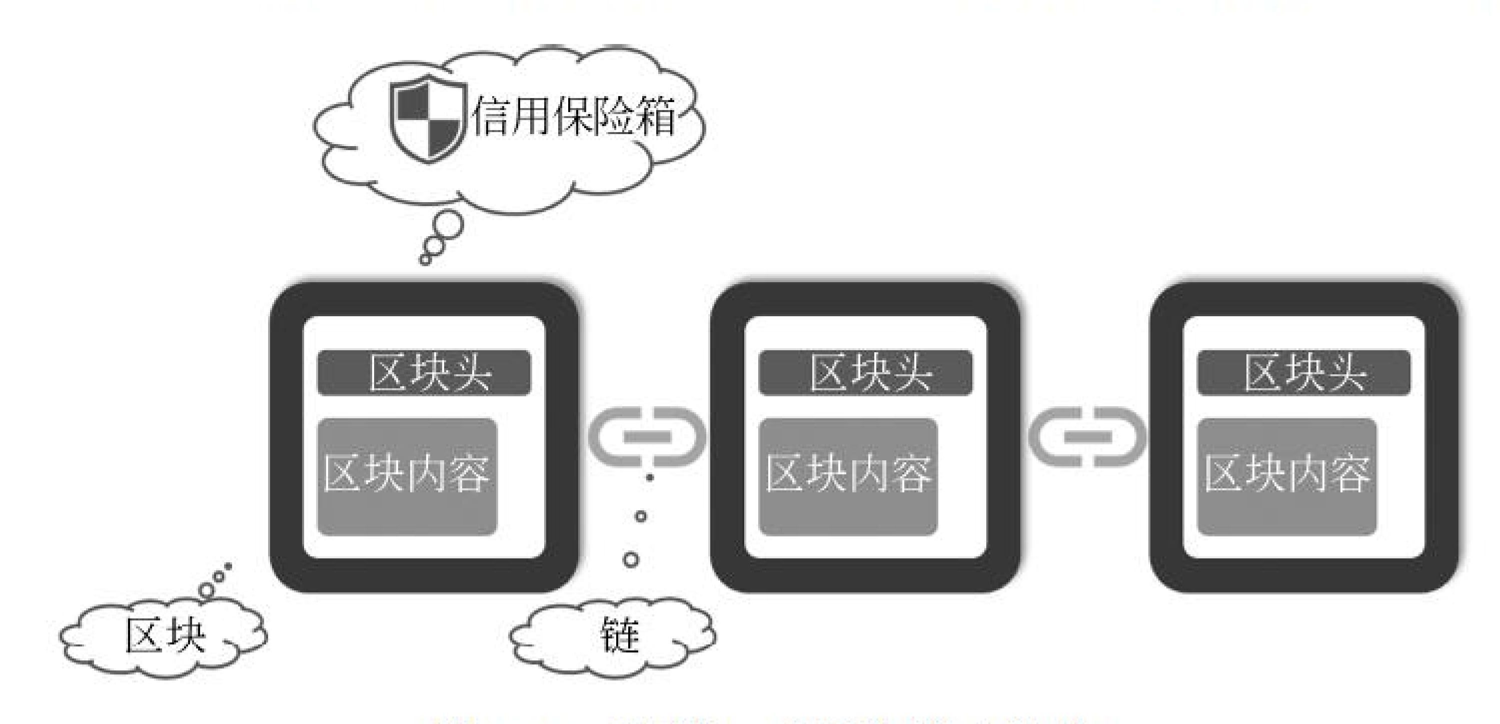


图 1.9　“区块 + 链”的账本结构

1.4　比特币交易

要对比特币交易进行介绍,我们首先要了解比特币地址的概念。要参与比特币系统中的交易过程,需要一个类似于现实世界中银行“账户”的实体。实际上,比特币的交易参与方实体为一组公私钥的组合,其中,私钥是由程序生成的一串随机数,而其公钥则是根据私钥经过一系列的计算生成的,公私钥之间存在一一对应的关系。其中,公钥作为参与交易的“账户名”,在交易中被引用,用于指明一笔交易中资金的来源及去向,而私钥则作为交易过程中的“验证密码”,用于确认某一交易的合法性。

如果以银行账户做个类比的话,一对比特币公私钥即相当于一个银行账户。其中公钥是公开的信息,它可以作为一个比特币账户对外的“账户名”,用于外界对该账户的引用,类似于银行账户的账号;相应地,比特币地址对应的私钥就相当于银行账户的密码,用于在转账时进行身份验证,从而保证用户的资金安全。

由于公私钥对为一个交易实体的唯一标记,所以需要保证各个用户所持有的比特币地址之间互不冲突,否则就可能出现安全问题。由于私钥本质上是随机生成的比特串,若有两个用户的私钥不巧是相同的,则一个用户完全可以用自己的私钥去替代另一个用户的私钥,从而使用另一个用户的资金。然而,在比特币的设计中,私钥的长度被设定为 256 比特,其可能的取值范围为$[0, 2^{256}-1]$,这是一个巨大的范围,可以认为与世界上沙子的数量相当,能够

保证在随机算法实现正确的情况下,基本不可能发生碰撞(生成两个完全相同的私钥)。这也是比特币乃至整个密码学的基础。

简单来说,比特币的一对公私钥以及其对应的钱包地址是按照如下的流程产生的:首先,通过某种随机数生成算法产生出一个 256 比特的比特串作为私钥,然后再使用椭圆曲线加密算法(Elliptic Curves Cryptography,ECC)对这个私钥计算生成公钥。此后,公钥再通过一系列的哈希计算和 Base58 编码得到钱包地址。

比特币交易即为从一个比特币地址向另一个比特币地址进行转账的过程,每个交易可能会包含多笔转账。

如图 1.10 所示,交易包含从比特币地址 1FzPNJ52ieWzvrcsSLUSgbEc2oBwczm4Ei 向比特币地址 19qM3R2YyhVf2HwcF2HocJsFXH6YZZDcSr 转 0.000 5 个比特币和向地址 19aEqa9UHVKqRLwsJ5Krq9VP4QV1AhBWVg 转 0.010 522 89 个比特币这两笔转账。交易输入的比特币中未被使用(转账给其他人)的剩余 0.003 136 个比特币则作为手续费,会被发送给挖出包含这个交易的区块的矿工,作为挖矿奖励的一部分。



图 1.10　比特币普通交易

资料来源:https://www.blockchain.com/zh-cn/btc/tx/a694c6725df984b9e9168f6cd5fa99171041766e0a01886a2232b84ba1e3709d

值得一提的是,上述我们提到的由 32 个字符组成的看似乱码的比特币地址,实际上是将其本身的 256 比特的比特串进行了编码,形成(相对于比特串)更为易读、易用的地址。

感兴趣的读者可以通过 https://www.blockchain.com/explorer 查看所有的比特币交易。

比特币交易有两种类型,一种是 Coinbase 交易,也就是挖矿奖励的比特币,这种交易没有发送人,例如图 1.11 所示的交易。另一种就是我们常见的普通交易了,即普通地址之间的转账交易,如图 1.10 中的交易。

比特币钱包是一个形象的概念,就是保存和管理比特币地址以及对应公私钥对的软件。根据终端类型的不同,比特币钱包可以分为桌面钱包、手机钱包、网页钱包和硬件钱包。不同



图 1.11　比特币 Coinbase 交易

资料来源：https://www.blockchain.com/zh-cn/btc/tx/788afccf6aba6802e39e36cbac93fdcfe953aea0d60c9b436dd9886f999d933a?show_adv = false

钱包的安全程度不同，对于少量比特币来说，选用网页钱包这种轻量级的钱包存储；而对于较大额度的比特币，建议使用更高级的钱包存储方式，比如硬件钱包，硬件钱包的成本最高，安全性也相对较高。

比特币官方提供钱包 Bitcoin Core，如图 1.12 所示，钱包中展示了可用的余额，可以给其他比特币地址转账、接收比特币并查看交易记录。



图 1.12　Bitcoin Core 界面

Bitcoin Core 是一个实现了全节点的比特币客户端，它的账本保存了 2009 年比特币面世以来所有的交易记录，这就意味着数据量大，全账本大小超过 185GB（截止到 2018 年 9 月底），全部同步要花几天时间（具体视电脑配置和网络环境而定）。当然通常我们没有必要下载整个账本，可以下载一个轻量版的钱包，比如 Electrum。完成安装及基础的网络、证书等配置工作后，即可使用，图 1.13 所示为其基本界面。

默认为历史界面（History），即与该钱包配置地址相关的转账记录。发送界面（Send）即转

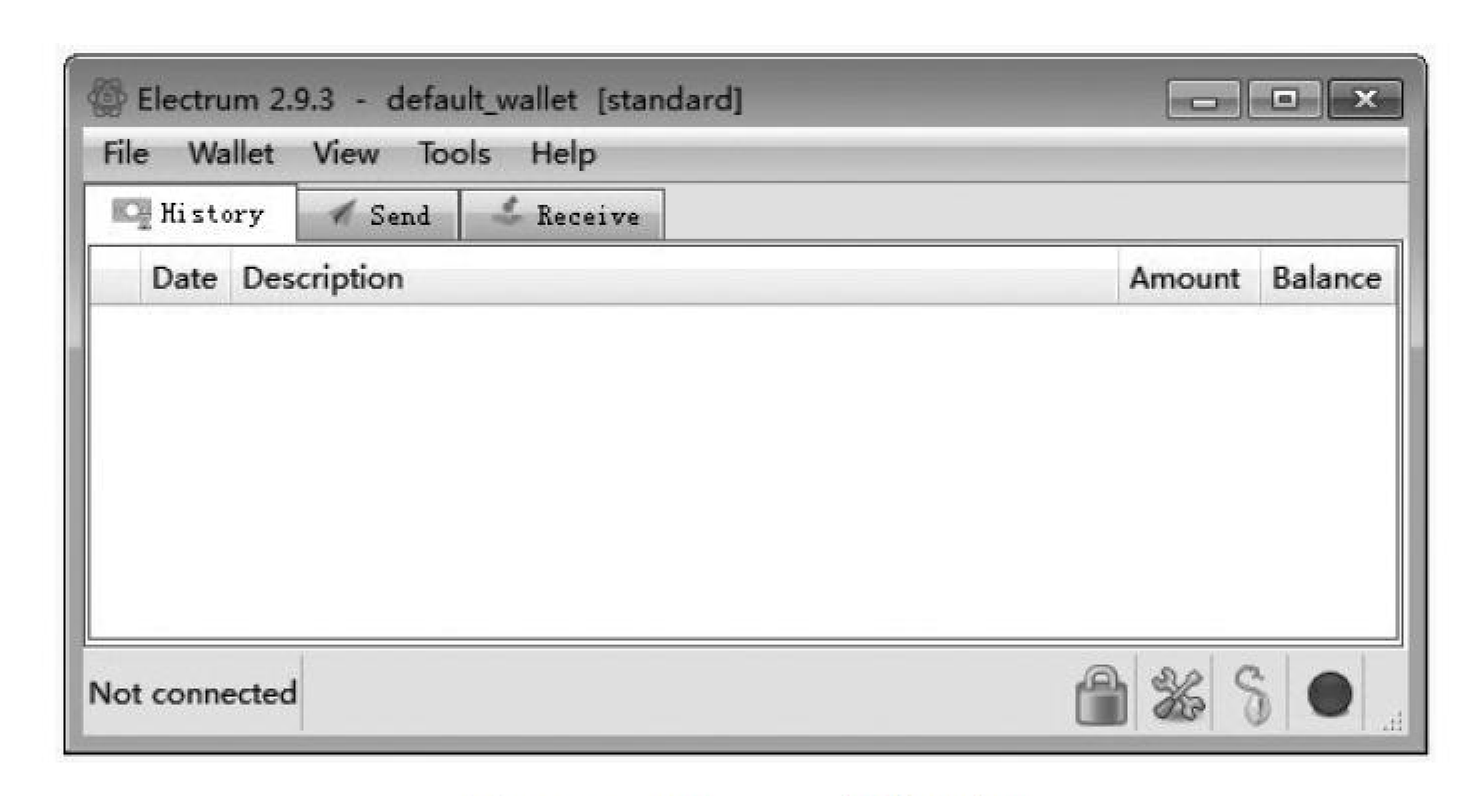


图 1.13　Electrum 操作界面

账给其他地址,填写目的地址、金额、说明、手续费等信息即可进行转账操作。接收界面(Receive)即为该钱包的收款地址,提供给他人后,对方即可转账至该地址。

除了上面的电脑版钱包外,还有网页版的钱包,以 https://blockchain.info 为代表,还有虚拟币交易网站的钱包也属于此类,这类钱包对币的控制权通过登录网站的用户名和密码保证。这种类型钱包使用最简便,当然安全性也是最低的。因为账户的私钥都是由网站保管的,这样理论上网站可以对用户的账户做任何操作。

如何获得比特币?获得比特币有 3 种途径。

(1) "矿工"挖矿所得;

(2) 线下通过中间人购买,线下支付法币或者任何等价物之后,转出方将比特币从他的地址转到购买者的地址,也可以通过线上"交易所"购买;

(3) 商家收取比特币,比如在本章开始提到佛罗里达程序员花 1 万个比特币购买比萨的店主就收到了比特币。

1.5　比特币挖矿

很长一段历史里作为基本货币的黄金,需要人工进行采矿获取,因此将比特币记账者们之间争抢激励的方式比作"挖矿"工作。当然比特币系统中挖矿只是一个形象的概念。比特币系统是一个参与节点互相验证的公开记账系统,而比特币挖矿的本质则是争夺某一个区块的记账权。

"挖矿"成功即是该节点成功获得当前区块记账权,也就是说其他节点就"照抄"该挖矿成功的节点的当前区块。获得记账权的节点会获取一定数量的比特币奖励,以此激励比特币网络中的所有节点积极参与记账工作。该奖励包含系统奖励和交易手续费两部分,系统奖励则作为比特币发行的手段。最初每生产一个"交易记录区块"可以获得 50 比特币的系统奖励,为控制比特币发行数量,该奖励每 4 年就会减半,到 2140 年即会基本发放完毕,最终整个

系统中最多只能有 2 100 万个比特币。

比特币系统大约每 10 分钟会记录一个数据块，这个数据块里包含了这 10 分钟内全网待确认的部分或全部交易。所谓的“挖矿”，就是争夺将这些交易打包成“交易记录区块”的权利。比特币系统会随机生成一道数学难题，后续会详细描述该数学难题，所有参与挖矿的节点一起参与计算这道数学难题，首先算出结果的节点将获得记账权。

每个节点会将过去一段时间内发生的、尚未经过网络公认的交易信息进行收集、检验、确认，最后打包并加签名为一个无法被篡改的“交易记录区块”，并在获得记账权后将该区块进行广播，从而让这个区块被全部节点认可，让区块中的交易成为比特币网络上公认已经完成的交易记录，永久保存。

1.5.1　挖矿的原理

挖矿最主要的工作就是计算上文提到的数学难题，最先求出解的矿工即可获得该块的记账权。在介绍这个数学难题前，先简单介绍一下哈希算法。哈希算法的基本功能概括来说，就是把任意长度的输入值通过一定的计算，生成一个固定长度的字符串，输出的字符串即为该输入的哈希值。比特币系统中采用 SHA-256 算法，该算法最终输出的哈希值长度为 256bit。由于此小节主要介绍挖矿原理，关于哈希算法的详细介绍请参见 2.2.1 小节，哈希运算的算法原理请参见 2.4.1 小节。

比特币中每个区块生成时，需要把上一个区块的哈希值、本区块的交易信息的默克尔树根、一个未知的随机数（nonce）拼在一起计算一个新的哈希值。为了保证 10 分钟产生一个区块，该工作必须具有一定难度，即哈希值必须以若干个 0 开头。哈希算法中，输入信息的任何微小改动即可引起哈希值的巨大变动，且这个变动不具有规律性。因为哈希值的位数是有限的，通过不断尝试随机数 nonce，总可以计算出一个符合要求的哈希值，且该随机数无法通过寻找规律计算出来。这意味着，该随机数只能通过暴力枚举的方式获得。挖矿中计算数学难题即为寻找该随机数的过程。

哈希值由 16 进制数字表示，即每一位有 16 种可能。根据哈希算法的特性，出现任何一个数字的概率是均等的，即每一位为“0”的概率为 1/16。要求某一位为“0”平均需要 16 次哈希运算，要求前 n 位为“0”，则需要进行哈希计算的平均次数为 16 的 n 次方。矿工为了计算出该随机数，需要花费一定的时间进行大量的哈希运算。

某个矿工成功计算出该随机数后，则会进行区块打包并全网广播。其他节点收到广播后，只需对包含随机数的区块按照同样的方法进行一次哈希运算即可，若哈希值以“0”开头的个数满足要求，且通过其他合法性校验，则接受这个区块，并停止本地对当前区块随机数的寻找，开始下个区块随机数的计算。

随着技术的发展，进行一次哈希计算速度越来越快，同时随着矿工的逐渐增多，算出满足哈希值以一定数量“0”开头的随机数的时间越来越短。为保证比特币始终按照平均每 10 分钟一个区块的速度出块，必须不断调整计算出随机哈希计算的平均次数，即调整哈希值以“0”

开头的数量要求,以此调整难度。比特币中,每生成 2 016 个区块就会调整一次难度,即调整周期大约为两周(2 016 × 10min = 14 天)。也就是说,对比生成最新 2 016 个区块花费的实际时间和按照每 10 分钟出一个块生成 2 016 个块的期望时间,若实际时间大于期望时间则降低难度,若实际时间小于期望时间则增加难度。

同时,为防止难度变化波动太大,每个周期调整幅度必须小于一个因子(当前为 4 倍)。若幅度大于 4 倍,则按照 4 倍调整。由于按照该幅度调整,出块速度仍然不满足预期,因此会在下一个周期继续调整。

1.5.2 矿池的原理

随着区块链的日渐火爆,参与挖矿的人越来越多,按照比特币原本的设计模式,只有成功打包一个区块的人才能获取奖励。如果每个矿工都独立挖矿,在如此庞大的基数下,挖矿成功的概率几乎为 0,只有一个幸运儿可以获取一大笔财富,其他矿工投入的算力、电力资源就会白白亏损。或许投入一台矿机,持续挖矿好几年甚至更久才能挖到一个区块。

为了降低这种不确定性,矿池应运而生。假如有 10 万矿工参与挖矿工作,这 10 万矿工的算力和占这个网络的 10%,则这 10 万个矿工中的某个矿工成功挖到下个块的概率即为 1/10。即平均每个矿工成功挖到下个区块的概率为 1/1 000 000,即平均每个矿工要花费 19 年可以成功挖到一个区块,然后获得相应的比特币奖励。这种挖矿模式风险过大,几乎没人可以承受。但是假设这 10 万个矿工共同协作参与挖矿,则平均每 100 分钟即可成功挖到一个区块,然后按照每个矿工提供的算力分配该次收益。这 10 万个矿工的收益也会趋于稳定。

当然上述只是对矿池原理进行一个简化的分析,实际情况则要复杂得多。当前大部分矿池是托管式矿池,一般由一个企业维护一个矿池服务器,运行专业的软件,协调矿池中矿工的计算任务。矿工不需要参与区块的验证工作,仅由矿池服务器验证即可,因此矿工也不需要存储历史区块,这极大地降低了矿工的算力及存储资源消耗。

协调矿工进行计算的思路也非常简单,矿池将打包区块需要的交易等信息验证完成后发送给矿工,然后降低矿工的挖矿难度。比如某个时段比特币系统需要哈希值“0”开头的个数大于 50 个,矿池可以将难度降低到 40 个“0”开头,矿工找到一个 40 个“0”开头哈希值的方案后,即可提交给矿池。矿池收到一个满足哈希值“0”开头个数大于 50 个的方案时,即可提交至比特币网络。当然,你也许会想:如果矿工计算得到一个“0”开头个数大于 50 的哈希值后,则直接提交给比特币网络,独享该区块的收益;如果计算得到一个“0”开头数在 40 到 50 之间的则提交到矿池,享受整个矿池分配的收益。该方案当然是行不通的,因为区块内容是由矿池发送给矿工的,即受益者地址已经包含在该区块中了,即使直接提交,最终受益的也是矿池。如果修改该地址,即意味着区块内容改变,则前面计算的哈希值也无效了。最后矿池按照矿工提交方案数量计算贡献的算力,最后根据算力分配收益。

当前矿池为协调矿工计算工作所采用的最为流行的协议为 Stratum 协议,该协议采用主动分配任务的方式。矿工首先需要连接到矿池订阅任务,矿池会返回订阅号 ID、矿池给矿工

指定的难度及后续构造区块所需要的信息。连接成功后，需要在矿池注册一个账户，添加矿工，每个账户可以添加多个矿工。注册完成后即可申请授权，矿池授权成功后才会给矿工分配任务。矿池分配任务时，会提供任务号 ID 及打包区块需要的相关信息。收到任务后，矿工即开始哈希计算并打包区块。如果矿工收到新任务，将直接终止旧任务，开始新任务，同时矿工也可以主动申请新任务。

这种托管式矿池一直饱受争议，矿池的存在大大降低了挖矿的门槛，使普通设备也可以参与到挖矿中，吸引更多矿工参与区块链网络，同时降低矿工的风险。但是弊病也非常明显，矿池的存在一定程度上违背了区块链去中心化的理念。于是有人提出了 P2P 矿池来取代托管式矿池，但是由于其效率远低于托管式矿池，收益低下，司马迁说的好："天下熙熙，皆为利来，天下攘攘，皆为利往。"大部分矿工都更愿意因为利益而选择托管式矿池。

由于托管式矿池掌握着大量的算力资源，拥有非常大的话语权，甚至某个矿池或者几个矿池联合掌握的算力超过整个网络的 50% 时，可以随意决定出块内容、双花等。但是也不用太过担心，从经济学的角度来讲，拥有大量算力的矿池，已经是既得利益者，为保障自己的利益，肯定会不遗余力地保障比特币网络的平稳运行。

1.6　比特币分叉

软件由于方案优化、BUG 修复等原因进行升级是一种非常常见的现象。如手机应用等传统软件，升级非常简单，只需厂商发布，用户接受升级即可。但是对于比特币这种去中心化的系统，升级是非常困难的，需要协调网络中每个参与者。软件升级意味着运行逻辑的改变，但是在比特币中，升级必然会导致不同节点在一定时间内运行不同的版本，于是就会产生分叉。

分叉主要包含软分叉和硬分叉两种。如果比特币升级后，新的代码逻辑向前兼容，即新规则产生的区块仍然会被旧节点接受，则为软分叉；如果新的代码逻辑无法向前兼容，即新产生的规则产生的区块无法被旧节点接受，则为硬分叉。

1. 软分叉

软分叉由于向前兼容，新旧节点仍然运行在同一条区块链上，并不会产生两条链，对整个系统影响相对较小。到目前为止，比特币发生过多次软分叉，如 BIP-34，BIP-65，BIP-66，BIP-9 等。其中比特币改进建议（Bitcoin Improvement Proposal，BIP）指的是比特币社区成员针对比特币提出的一系列改进建议，这些改进建议的具体内容感兴趣的读者可以通过访问 BIP 的网站①自行查阅。

此处以 BIP-34 为例，简单说明软分叉的过程。在旧版本中，存在一个无意义的字段"coinbase data"，矿工不会去验证该字段的内容。BIP-34 升级的新版本则要求该字段必须包含区块高度，同时将版本信息由"1"修改为"2"。该升级共包含三个阶段。

---

①　地址：https://github.com/bitcoin/bips。

第一个阶段：矿工将版本号修改为“2”，此时所有矿工验证区块时，按照旧的规则验证，即不关心“coinbase data”字段内容，所有矿工不论以新规则还是旧规则打包区块，均可以被整个网络接受。

第二阶段：如果最新产生的1 000个区块中，版本号为“2”的区块个数超过75%时，则要求版本号为“2”的矿工必须按照新的规则打包区块，升级的矿工收到版本号为“2”的区块时，只会接受“coinbase data”字段包含区块高度的区块，对于版本号为“1”的区块，仍然不校验该字段并接受。

第三阶段：如果最新产生的1 000个区块中，版本号为“2”的区块个数超过95%，则升级的矿工只接受版本号为“2”的区块，并会对“coinbase data”字段进行校验，版本号为“1”的区块则不被接受，以此来逼迫剩余少量矿工进行升级。

软分叉虽然对系统的影响较小，但是为了保证向前兼容，不能新增字段，只能在现有数据结构下修改，即可升级的内容非常有限。同时，因为这些限制，软分叉一般升级方案比较复杂，复杂的方案往往更容易产生BUG，并且可维护性很差。

2. 硬分叉

硬分叉相比软分叉则会“暴力”很多，由于不向前兼容，旧版本矿工无法验证新版本的区块而拒绝接受，仍然按照旧的逻辑只接受旧版本矿工打包的区块。而新版本产生的区块则会被新版本矿工接受，因此新版本矿工保存的区块会和旧版本矿工保存的区块产生差别，即会形成两条链。

硬分叉修改余地很大，方案设计比较简单，但是如果整个网络中有两种不同的意见，就会导致整个生态的分裂。当前比特币影响最广泛的硬分叉事件即为2017年8月1日的硬分叉，比特币由一条链分叉产生一条新的链“比特现金（Bitcoin Cash，BCH）”。

这次硬分叉的起因是开发者与矿工在比特币扩容方案上的分歧。比特币区块大小为1MB，按照每10分钟一个区块的速度，全球每秒只能完成大约7笔交易。比特币发展初期，1MB的区块足够打包出块间隔内产生的所有交易，但是在比特币如此火爆的今天，这种处理速度显然达不到要求。一笔交易往往需要等待数个小时甚至更久，当前比特币网络已经有大约几十万交易排队等待打包确认。比特币交易可以支付手续费（不强制要求），由于矿工逐利的属性，矿工在打包区块时，往往会选择手续费更高的交易打包。这意味着，如果不想排队，则需要支付更高的手续费，以期望获得优先处理权。而过高的手续费显然违背了比特币的设计初衷。

为了解决以上问题，经过社区讨论，最终形成了两个改进方案，分别是扩容方案和隔离见证方案。

扩容方案的想法比较直接，既然现在因为区块太小而导致交易处理速度低下，那就直接扩大区块的容量，使其能容纳更多的交易。原来1MB不够用，那么就扩成2MB、8MB，甚至直接扩到32MB。

隔离见证方案的想法是，将交易分为两部分，一部分是交易信息，另一部分是见证信息，

这两部分信息分开进行处理。好比一辆车太小,要搭车的人太多,于是让车上所有人将背包和行李放在另一辆跟着的货车上,这样原来的车就可以容纳更多的人了。

支持扩容方案的主要是矿工们。矿工们认为交易的高效才是最重要的,这样才能体现比特币的世界货币价值。矿工的利益来源于挖矿,如果比特币交易处理吞吐量较低,用户为使自己的交易尽早得到打包处理会倾向于向矿工提供更高的手续费,矿工因此可以获得超额手续费,其短期收益是增加的。但长期来看,只有比特币价格维持上涨,挖矿的收益才会持续提升。因而,从长远考虑,扩容是必须的,毕竟只有比特币交易更加顺畅,入场人数增多,资金盘越来越大,矿工的收益才会获得显著增长。采用扩容方案,矿工可以在每个区块中包含更多的交易,从而获取更多的手续费,然而若使用隔离见证的扩容方案,小额的交易将不通过区块确认,矿工的手续费收益会大幅降低,因此矿工更倾向于支持扩容方案。

隔离见证方案的支持者主要是比特币开发团队的部分核心成员。他们认为,扩容方案是一个“扬汤止沸”的方案,毕竟不可能无限制地对区块的容量进行扩大。同时,区块的变大会使得挖矿的门槛提高,从而降低普通矿工的参与度,导致比特币系统的去中心化程度减弱。

2016 年 2 月和 2017 年 3 月,争议双方两次进行商讨,希望双方各退一步,接受一个折中的方案,该方案中,区块容量将会被扩大到 2MB,同时也对比特币部署隔离见证的方案。但是,由于期间有参与方反悔或者反对,导致最终没有达成共识,这也给“硬分叉”埋下了伏笔。

在 2017 年 8 月 1 日,比特大陆投资的矿池 ViaBTC 团队,采用比特大陆提出的 UAHF(用户激活的硬分叉)方案,挖出了第一个区块,对比特币区块链进行了硬分叉。自此,与比特币竞争的分叉币比特币现金诞生。比特币现金区块链的区块容量达到了 8MB,且没有采用隔离见证方案。

1.7 比特币类加密数字货币

比特币的流行刺激了全球对于发行电子货币的热情,各式各样的加密数字货币涌现出来。目前全球发行的加密数字货币有两千多种,比如比特币、比特现金、以太币、瑞波币、恒星币等,各种加密数字货币市值和影响力不尽相同。很多加密数字货币源自比特币或者以太坊源代码的克隆,也有一些针对特定问题构建了独特解决方案的加密数字货币,从应用场景和技术的角度来讲有一定的创新性,比如:莱特币(LTC)、质数币(XPM)、Zcash、门罗币等。这些币在加密数字货币方面的应用外,也给区块链技术的发展做出了很大的贡献,提供了很多新的思路。

莱特币(Litecoin,LTC)受到了比特币(BTC)的启发,并且在技术上具有相同的实现原理。莱特币旨在改进比特币,与其相比,莱特币具有三种显著差异:第一,莱特币网络每 2.5 分钟(而不是 10 分钟)就可以处理一个块,因此可以提供更快的交易确认;第二,莱特币网络预期产出 8 400 万个莱特币,是比特币网络发行货币量的 4 倍之多;第三,莱特币在其工作量证明算法中使用了由 Colin Percival 提出的 scrypt 加密算法,这使得相对于比特币,在普通计算机上

进行莱特币挖掘更为容易。每一个莱特币被分成100 000 000个更小的单位,通过8位小数来界定。

质数币(Primecoin,XPM)号称拥有科研价值和现实意义。质数币仍然使用PoW机制,它挖矿的过程就是寻找质数链。质数在数论领域具有极高价值,质数币是一种使挖矿过程中消耗的大量能源产生价值的加密数字货币。

Zcash是首个使用零知识证明机制的区块链系统。零知识证明简单点讲,就是证明者能够在不向验证者提供任何有用的信息的情况下,使验证者相信某个论断是正确的,所以Zcash可提供完全的支付保密性。Zcash是比特币的分支,保留了比特币原有的模式,不同之处在于,Zcash交易能够自动隐藏区块链上所有交易的发送者、接受者及数额。只有那些拥有查看密钥的人才能看到交易的内容。用户拥有完全的控制权,他们可自行选择向其他人提供查看密钥。

门罗币(Monero,XMR)是另一个比较流行的隐私保护的加密数字货币,它同样具有隐藏地址、保护用户的隐私与匿名的功能。与Zcash不同,门罗币采用环签名方式保护用户隐私。环签名环中一个成员利用他的私钥和其他成员的公钥进行签名,但却不需要征得其他成员的允许,而验证者只知道签名来自这个环,但不知道谁是真正的签名者,这个方式解决了对签名者完全匿名的问题。

1.8 本章小结

本章作为本书的第一章,以比特币作为起点带领读者进入区块链的世界。对于刚开始接触区块链知识的读者来说,了解比特币的发展历史能够很好地帮助理解区块链的基础思想,而且第三节也以故事的形式通俗地讲解了比特币的原理。除了这些基础知识,本章还对比特币的交易、挖矿和分叉等概念进行了进一步的讨论,使得读者能够全面地了解比特币。本章最后还扩展介绍了类似于比特币的其他加密数字货币,让读者由点及面地了解比特币相关的信息。以加密数字货币作为入口,读者能够更好地开启学习了解区块链技术的旅程。

需要郑重声明的是,本章主要目的是从技术的角度介绍当前较有特色的一些数字货币,并不代表笔者认可这些数字货币(及后续章节涉及的数字货币)的价格,希望读者能基于本章以及本书其他章节对数字货币的价值有一个自己的认识,也希望读者能正确地认识到其中存在的风险。同时对于本书提到的一些数字货币交易平台仅仅是为了介绍当前的生态,不代表笔者为其资质背书。

第2章
区块链技术原理

从2009年比特币问世至今,区块链已经走过了第一个十年。十年间,区块链逐步进入大众视野,尤其是在单枚比特币的价格被炒作到近2万美元以后,整个社会对于比特币的关注度急剧上升。一方面,乱象丛生的自媒体流传着各种“币圈”暴富神话,各种鱼龙混杂的区块链项目浮出水面,其中不乏打着区块链技术创新名号,实则通过ICO融资圈钱的低质量项目。另一方面,区块链技术本身吸引了越来越多的人对其进行深入研究并探索其宽广的应用空间:各地政府对区块链积极扶持,国内外科技及金融巨头纷纷涉足区块链行业。区块链究竟是一门怎样的技术,竟有如此魅力。俗话说,外行看热闹,内行看门道,让我们来一探究竟。

2.1 区块链的概念

那么到底什么是区块链呢?工信部指导发布的《区块链技术和应用发展白皮书2016》的解释是:狭义来讲,区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构,并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义来讲,区块链技术是利用块链式数据结构来验证和存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全性、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

专业的解释或许有些拗口。顾名思义,区块链(blockchain)是一种数据以区块(block)为单位产生和存储,并按照时间顺序首尾相连形成链式(chain)结构,同时通过密码学保证不可篡改、不可伪造及数据传输访问安全的去中心化分布式账本。区块链中所谓的账本,其作用和现实生活中的账本基本一致,按照一定的格式记录流水等交易信息。特别是在各种数字货币中,交易内容就是各种转账信息。只是随着区块链的发展,记录的交易内容由各种转账记录扩展至各个领域的数据。比如,在供应链溯源应用中,区块中记录了供应链各个环节中物品所处的责任方、位置等信息。

要探寻区块链的本质,什么是区块、什么是链,首先需要了解区块链的数据结构,即这些交易以怎样的结构保存在账本中。区块是链式结构的基本数据单元,聚合了所有交易相关信息,主要包含区块头和区块主体两部分。区块头主要由父区块哈希值(Previous Hash)、时间戳(Timestamp)、默克尔树根(Merkle Tree Root)等信息构成;区块主体一般包含一串交易的列表。每个区块中的区块头所保存的父区块的哈希值,便唯一地指定了该区块的父区块,在区块间构成了连接关系,从而组成了区块链的基本数据结构。

总的来说,区块链的数据结构示意图如图 2.1 所示。本章的后续小节将对区块链如何利用其数据结构以及基础技术来达成区块链的特性进行介绍。

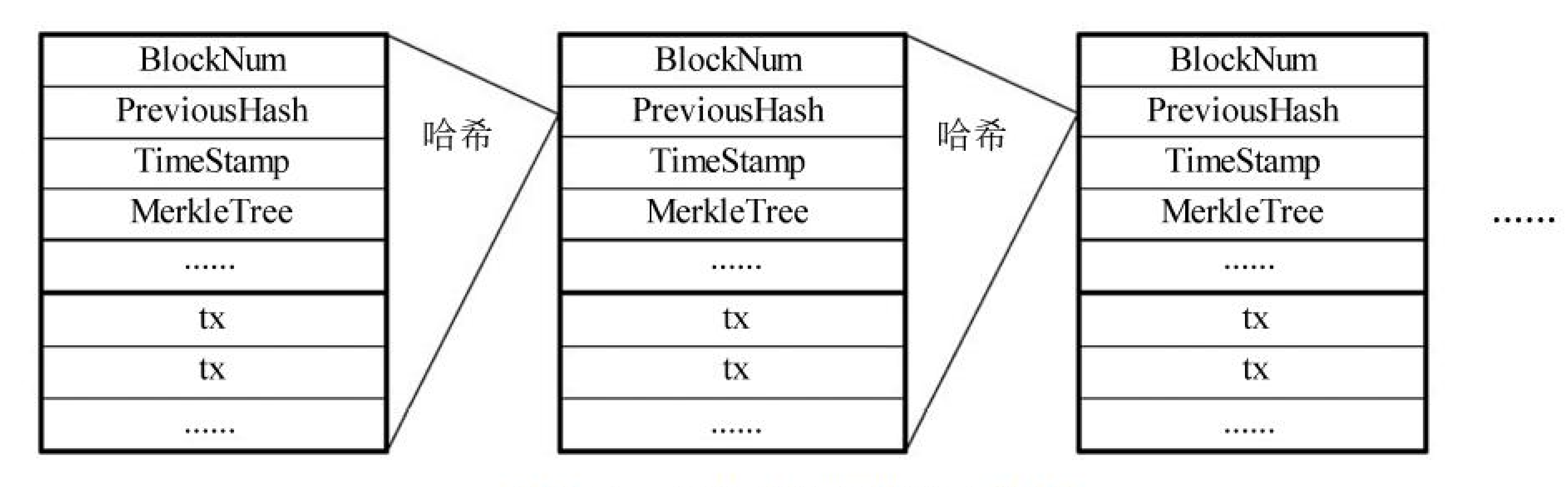


图 2.1 区块链数据结构示意图

2.2 区块链基础技术

区块链作为一个诞生刚到十年的技术,的确算是一个新兴的概念,但是它所用到的基础技术全是当前非常成熟的技术。区块链的基础技术如哈希运算、数字签名、P2P 网络、共识算法以及智能合约等,在区块链兴起之前,很多技术已经在各种互联网应用中被广泛使用。但这并不意味着区块链就是一个新瓶装旧酒的东西。就好比积木游戏,虽然是一些简单有限的木块,但是组合过后,就能创造出一片新的世界。同时,区块链也并不是简单的重复使用现有技术,例如共识算法、隐私保护在区块链中已经有了很多的革新,智能合约也从一个简单的理念变成了一个现实。区块链“去中心化”或“多中心”这种颠覆性的设计思想,结合其数据不可篡改、透明、可追溯、合约自动执行等强大能力,足以掀起一股新的技术风暴。本小节主要

探讨这些技术的原理及在区块链系统中的作用。

2.2.1　哈希运算

区块链账本数据主要通过父区块哈希值组成链式结构来保证不可篡改性。下面我们分别看什么是哈希运算、哈希运算的特性以及哈希运算在区块链系统中的作用。我们以比特币系统中的第 549 660 个区块(如图 2.2 所示)为例看哈希运算都用在了什么地方。

Block #549660

Summary	
Number Of Transactions	2170
Output Total	5,653.55907964 BTC
Estimated Transaction Volume	772.70702429 BTC
Transaction Fees	0.15997469 BTC
Height	549660 (Main Chain)
Timestamp	2018-11-11 13:46:38
Received Time	2018-11-11 13:46:38
Relayed By	BTC.TOP
Difficulty	7,184,404,942,701.79
Bits	388443538
Size	1314.646 kB
Weight	3992.629 kWU
Version	0x20000000
Nonce	3443302353
Block Reward	12.5 BTC

Hashes	
Hash	0000000000000000000e1759fab62e4ededd9ea0ae990a7753a237cad92b74fc
Previous Block	0000000000000000001f7331308a74960324000389dd46f4e96a9d73da1af0ce
Next Block(s)	00000000000000000026b14ede1c83d3f852baaffd5f136f1a85aea629d1bb62
Merkle Root	374c2feedda09d31cbf4f60bcc48057e5e0f4bd7c22d772a91bd0e8a0df07d3a

图 2.2　比特币系统第 549 660 个区块部分数据

图片来源于 https://www.blockchain.com/btc/block-index/1732212

1. 什么是哈希运算

哈希算法(Hash Algorithm)即散列算法的直接音译。它的基本功能概括来说,就是把任意长度的输入(例如文本等信息)通过一定的计算,生成一个固定长度的字符串,输出的字符串称为该输入的哈希值。在此以常用的 SHA-256 算法分别对一个简短的句子和一段文字求哈希值来说明。

- 输入:This is a hash example!
  哈希值:f7f2cf0bcbfbc11a8ab6b6883b03c721407da5c9745d46a5fc53830d4749504a
- 输入:此处以比特币白皮书英文原版摘要部分作为输入
  A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending

problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

哈希值：3143293acc4a9692a3db8460b24f6c0777dbbed03909ad8eeb27849039a5113b

2. 哈希运算的特性

一个优秀的哈希算法要具备正向快速、输入敏感、逆向困难、强抗碰撞等特征。

- 正向快速：正向即由输入计算输出的过程，对给定数据，可以在极短时间内快速得到哈希值。如当前常用的SHA256算法在普通计算机上一秒钟能做2 000万次哈希运算。
- 输入敏感：输入信息发生任何微小变化，哪怕仅仅是一个字符的更改，重新生成的哈希值与原哈希值也会有天壤之别。同时完全无法通过对比新旧哈希值的差异推测数据内容发生了什么变化。因此，通过哈希值可以很容易地验证两个文件内容是否相同。该特性广泛应用于错误校验。在网络传输中，发送方在发送数据的同时，发送该内容的哈希值。接收方收到数据后，只需要将数据再次进行哈希运算，对比输出与接收的哈希值，就可以判断数据是否损坏。
- 逆向困难：要求无法在较短时间内根据哈希值计算出原始输入信息。该特性是哈希算法安全性的基础，也因此是现代密码学的重要组成。哈希算法在密码学中的应用很多，此处仅以哈希密码举例进行说明。当前生活离不开各种账户和密码，但并不是每个人都有为每个账户单独设置密码的好习惯，为了记忆方便，很多人的多个账户均采用同一套密码。如果这些密码原封不动地保存在数据库中，一旦数据泄露，则该用户所有其他账户的密码都可能暴露，造成极大风险。所以在后台数据库仅会保存密码的哈希值，每次登录时，计算用户输入的密码的哈希值，并将计算得到的哈希值与数据库中保存的哈希值进行比对。由于相同输入在哈希算法固定时，一定会得到相同的哈希值，因此只要用户输入密码的哈希值能通过校验，用户密码即得到了校验。在这种方案下，即使数据泄露，黑客也无法根据密码的哈希值得到密码原文，从而保证了密码的安全性。
- 强抗碰撞性：即不同的输入很难可以产生相同的哈希输出。当然，由于哈希算法输出位数是有限的，即哈希输出数量是有限的，而输入却是无限的，所以不存在永远不发生碰撞的哈希算法。但是哈希算法仍然被广泛使用，只要算法保证发生碰撞的概率

够小,通过暴力枚举获取哈希值对应输入的概率就更小,代价也相应更大。只要能保证破解的代价足够大,那么破解就没有意义。就像我们购买双色球时,虽然我们可以通过购买所有组合保证一定中奖,但是付出的代价远大于收益。优秀的哈希算法即需要保证找到碰撞输入的代价远大于收益。

哈希算法的以上特性,保证了区块链的不可篡改性。对一个区块的所有数据通过哈希算法得到一个哈希值,而这个哈希值无法反推出原来的内容。因此区块链的哈希值可以唯一、准确地标识一个区块,任何节点通过简单快速地对区块内容进行哈希计算都可以独立地获取该区块哈希值。如果想要确认区块的内容是否被篡改,利用哈希算法重新进行计算,对比哈希值即可确认。

3. 通过哈希构建区块链的链式结构,实现防篡改

每个区块头包含了上一个区块数据的哈希值,这些哈希层层嵌套,最终将所有区块串联起来,形成区块链。区块链里包含了自该链诞生以来发生的所有交易,因此,要篡改一笔交易,意味着它之后的所有区块的父区块哈希全部要篡改一遍,这需要进行大量的运算。如果想要篡改数据,必须靠伪造交易链实现,即保证在正确的区块产生之前能快速地运算出伪造的区块。同时在以比特币为代表的区块链系统要求连续产生一定数量的区块之后,交易才会得到确认,即需要保证连续伪造多个区块。只要网络中节点足够多,连续伪造的区块运算速度都超过其他节点几乎是不可能实现的。另一种可行的篡改区块链的方式是,某一利益方拥有全网超过 50% 的算力,利用区块链中少数服从多数的特点,篡改历史交易。然而在区块链网络中,只要有足够多的节点参与,控制网络中 50% 的算力也是不可能做到的。即使某一利益方拥有了全网超过 50% 的算力,那已经是既得利益者,肯定会更坚定地维护区块链网络的稳定性。

4. 通过哈希构建默克尔树,实现内容改变的快速检测

除上述防篡改特性,基于哈希算法组装出的默克尔树也在区块链中发挥了重要作用。默克尔树本质上是一种哈希树,1979 年瑞夫 · 默克尔申请了该专利,故此得名。前面已经介绍了哈希算法,在区块链中默克尔树就是当前区块所有交易信息的一个哈希值。但是这个哈希值并不是直接将所有交易内容计算得到的哈希,而是一个哈希二叉树。首先对每笔交易计算哈希值;然后进行两两分组,对这两个哈希值再计算得到一个新的哈希值,两个旧的哈希值就作为新哈希值的叶子节点,如果哈希值数量为单数,则对最后一哈希值再次计算哈希值即可;然后重复上述计算,直至最后只剩一个哈希值,作为默克尔树的根,最终形成一个二叉树的结构。

在区块链中,我们只需要保留对自己有用的交易信息,删除或者在其他设备备份其余交易信息。如果需要验证交易内容,只需验证默克尔树即可。若根哈希验证不通过,则验证两个叶子节点,再验证其中哈希验证不通过的节点的叶子节点,最终可以准确识别被篡改的交易。

默克尔树在生活中其他领域应用也非常广泛。例如 BT 下载,数据一般会分成很多个小块,以保证快速下载。在下载前,先下载该文件的一个默克尔树,下载完成后,重新生成默克尔树进行对比校验。若校验不通过,可根据默克尔树快速定位损坏的数据块,重新下载即可。

2.2.2 数字签名

1. 数字签名的作用

日常生活中我们手写的签名相信大家都不陌生,作为确定身份、责任认定的重要手段,各种重要文件、合同等均需要签名确认。同一个字,不同的人写出来虽然含义完全相同,但是字迹这种附加值是完全不同的,刻意模仿也能通过专业的手段进行鉴别。因为签名具有唯一性,所以可以通过签名来确定身份及定责。

区块链网络中包含大量的节点,不同节点的权限不同。举个简单的例子,就像现实生活中只能将自己的钱转给他人,而不能将别人的钱转给自己,区块链中的转账操作,必须要由转出方发起。区块链主要使用数字签名来实现权限控制,识别交易发起者的合法身份,防止恶意节点身份冒充。

2. 数字签名的效力

数字签名也称作电子签名,是通过一定算法实现类似传统物理签名的效果。目前已经有包括欧盟、美国和中国等在内的 20 多个国家和地区认可数字签名的法律效力。2000 年,中国新的《合同法》首次确认了电子合同、数字签名的法律效力。2005 年 4 月 1 日,中国首部《电子签名法》正式实施。数字签名在 ISO 7498-2 标准中定义为:“附加在数据单元上的一些数据,或是对数据单元所做的密码变换,这种数据和变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性,并保护数据,防止被人(例如接收者)进行伪造。”

3. 数字签名的原理

这里要澄清一个误区,即数字签名并不是指通过图像扫描、电子板录入等方式获取物理签名的电子版,而是通过密码学领域相关算法对签名内容进行处理,获取一段用于表示签名的字符。在密码学领域,一套数字签名算法一般包含签名和验签两种运算,数据经过签名后,非常容易验证完整性,并且不可抵赖。只需要使用配套的验签方法验证即可,不必像传统物理签名一样需要专业手段鉴别。数字签名通常采用非对称加密算法,即每个节点需要一对私钥、公钥密钥对。所谓私钥即只有本人可以拥有的密钥,签名时需要使用私钥。不同的私钥对同一段数据的签名是完全不同的,类似物理签名的字迹。数字签名一般作为额外信息附加在原消息中,以此证明消息发送者的身份。公钥即所有人都可以获取的密钥,验签时需要使用公钥。因为公钥人人可以获取,所以所有节点均可以校验身份的合法性。

数字签名的流程如下:

- 发送方 A 对原始数据通过哈希算法计算数字摘要,使用非对称密钥对中的私钥对数字摘要进行加密,这个加密后的数据就是数字签名;

- 数字签名与 A 的原始数据一起发送给验证签名的任何一方。

验证数字签名的流程如下：

- 首先，签名的验证方，一定要持有发送方 A 的非对称密钥对的公钥；
- 在接收到数字签名与 A 的原始数据后，首先使用公钥，对数字签名进行解密，得到原始摘要值；
- 然后，对 A 的原始数据通过同样的哈希算法计算摘要值，进而比对解密得到的摘要值与重新计算的摘要值是否相同，如果相同，则签名验证通过。

A 的公钥可以解密数字签名，保证了原始数据确实来自 A；解密后的摘要值，与原始数据重新计算得到的摘要值相同，保证了原始数据在传输过程中未经过篡改。签名及签名验证的流程如图 2.3 所示。

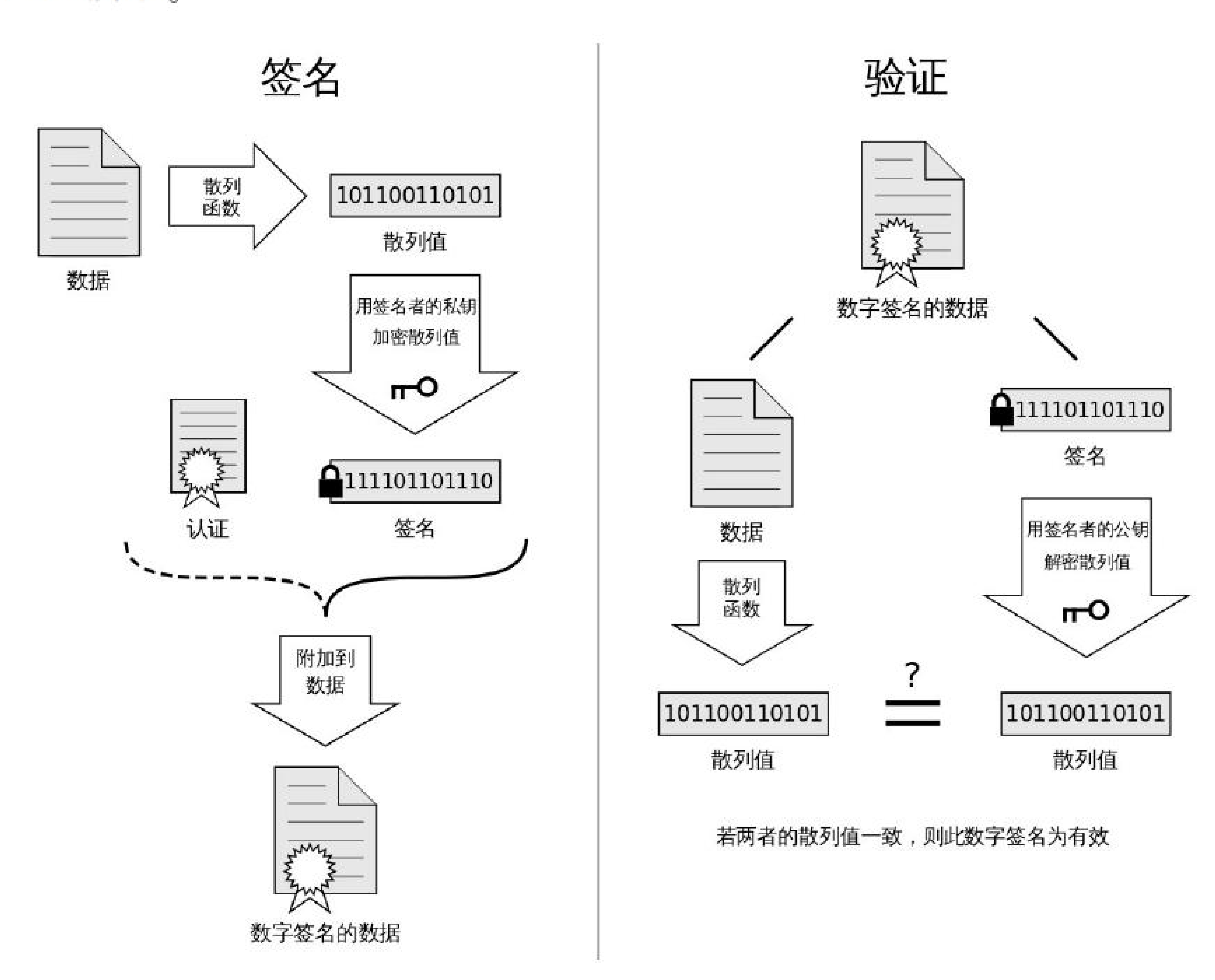


图 2.3　签名及签名验证的流程示意图

资料来源：https://zh.wikipedia.org/wiki

4. 区块链中的用法

在区块链网络中，每个节点都拥有一份公私钥对。节点发送交易时，先利用自己的私钥对交易内容进行签名，并将签名附加在交易中。其他节点收到广播消息后，首先对交易中附加的数字签名进行验证，完成消息完整性校验及消息发送者身份合法性校验后，该交易才会触发后续处理流程。这对应到前文"比特币的通俗故事"一节中村民验证喊出交易者的声音，确保是张三自己发出的交易。

2.2.3 共识算法

1. 为什么要共识?

区块链通过全民记账来解决信任问题,但是所有节点都参与记录数据,那么最终以谁的记录为准?或者说,怎么保证所有节点最终都记录一份相同的正确数据,即达成共识?在传统的中心化系统中,因为有权威的中心节点背书,因此可以以中心节点记录的数据为准,其他节点仅简单复制中心节点的数据即可,很容易达成共识。然而在区块链这样的去中心化系统中,并不存在中心权威节点,所有节点对等地参与到共识过程之中。由于参与的各个节点的自身状态和所处网络环境不尽相同,而交易信息的传递又需要时间,并且消息传递本身不可靠,因此,每个节点接收到的需要记录的交易内容和顺序也难以保持一致。更不用说,由于区块链中参与的节点的身份难以控制,还可能会出现恶意节点故意阻碍消息传递或者发送不一致的信息给不同节点,以干扰整个区块链系统的记账一致性,从而从中获利的情况。因此,区块链系统的记账一致性问题,或者说共识问题,是一个十分关键的问题,它关系着整个区块链系统的正确性和安全性。

2. 有哪些共识算法?

当前区块链系统的共识算法有许多种,主要可以归类为如下四大类:(1)工作量证明(Proof of Work,PoW)类的共识算法;(2)Po * 的凭证类共识算法;(3)拜占庭容错(Byzantine Fault Tolerance,BFT)类算法;(4)结合可信执行环境的共识算法。接下来本节将分别对这四类算法进行简要的介绍。

- PoW 类的共识算法

PoW 类的共识算法主要包括区块链鼻祖比特币所采用的 PoW 共识及一些类似项目(如莱特币等)的变种 PoW,即为大家所熟知的“挖矿”类算法。这类共识算法的核心思想实际是所有节点竞争记账权,而对于每一批次的记账(或者说,挖出一个区块)都赋予一个“难题”,要求只有能够解出这个难题的节点挖出的区块才是有效的。同时,所有节点都不断地通过试图解决难题来产生自己的区块并将自己的区块追加在现有的区块链之后,但全网络中只有最长的链才被认为是合法且正确的。

比特币类区块链系统采取这种共识算法的巧妙之处在于两点:首先,它采用的“难题”具有难以解答,但很容易验证答案的正确性的特点,同时这些难题的“难度”,或者说全网节点平均解出一个难题所消耗时间,是可以很方便地通过调整难题中的部分参数来进行控制的,因此它可以很好地控制链增长的速度。同时,通过控制区块链的增长速度,它还保证了若有一个节点成功解决难题完成了出块,该区块能够以(与其他节点解决难题速度相比)更快的速度在全部节点之间传播,并且得到其他节点的验证的特性;这个特性再结合它所采取的“最长链有效”的评判机制,就能够在大多数节点都是诚实(正常记账出块,认同最长链有效)的情况下,避免恶意节点对区块链的控制。这是因为,在诚实节点占据了全网 50% 以上的算力比例时,从期望上讲,当前最长链的下一个区块很大概率也是诚实节点生成的,并且该诚实节点一

旦解决了“难题”并生成了区块,就会在很快的时间内告知全网其他节点,而全网的其他节点在验证完毕该区块后,便会基于该区块继续解下一个难题以生成后续的区块,这样以来,恶意节点很难完全掌控区块的后续生成。

PoW 类的共识算法所设计的“难题”一般都是需要节点通过进行大量的计算才能够解答的,为了保证节点愿意进行如此多的计算从而延续区块链的生长,这类系统都会给每个有效区块的生成者以一定的奖励。比特币中解决的难题即寻找一个符合要求的随机数,具体解决方法详见本书 1.5 小节的介绍。在如图 2.2 展示的区块数据中,左侧“Nonce”字段即为该区块对应难题的解,即该区块符合要求的随机数为“3443302353”。

然而不得不承认的是,PoW 类算法给参与节点带来的计算开销,除了延续区块链生长外无任何其他意义,却需要耗费巨大的能源,并且该开销会随着参与的节点数目的上升而上升,是对能源的巨大浪费。

- Po * 的凭证类共识算法

鉴于 PoW 的缺陷,人们提出了一些 PoW 的替代者——Po * 类算法。这类算法引入了“凭证”的概念(即 Po * 中的 *,代表各种算法所引入的凭证类型):根据每个节点的某些属性(拥有的币数、持币时间、可贡献的计算资源、声誉等),定义每个节点进行出块的难度或优先级,并且取凭证排序最优的节点,或是取凭证最高的小部分节点进行加权随机抽取某一节点,进行下一段时间的记账出块。这种类型的共识算法在一定程度上降低了整体的出块开销,同时能够有选择地分配出块资源,即可根据应用场景选择“凭证”的获取来源,是一个较大的改进。然而,凭证的引入提高了算法的中心化程度,一定程度上有悖于区块链“去中心化”的思想,且多数该类型的算法都未经过大规模的正确性验证实验,部分该类算法的矿工激励不够明确,节点缺乏参与该类共识的动力。

- BFT 类算法

无论是 PoW 类算法还是 Po * 类算法,其中心思想都是将所有节点视作竞争对手,每个节点都需要进行一些计算或提供一些凭证来竞争出块的权利(以获取相应的出块好处)。BFT 类算法则采取了不同的思路,它希望所有节点协同工作,通过协商的方式来产生能被所有(诚实)节点认可的区块。

拜占庭容错问题最早由 Leslie Lamport 等学者于 1982 年在论文 *The Byzantine Generals Problem* 中正式提出,主要描述分布式网络节点通信的容错问题。从 20 世纪 80 年代起,提出了很多解决该问题的算法,这类算法被统称为 BFT 算法。实用拜占庭容错(Practical BFT, PBFT)算法是最经典的 BFT 算法,由 Miguel Castro 和 Barbara Liskov 于 1999 年提出。PBFT 算法解决了之前 BFT 算法容错率较低的问题,且降低了算法复杂度,使 BFT 算法可以实际应用于分布式系统。PBFT 在实际分布式网络中应用非常广泛,随着当前区块链的迅速发展,很多针对具体场景的优化 BFT 算法不断涌现。

具体地,BFT 类共识算法一般都会定期选出一个领导者,由领导者来接收并排序区块链系统中的交易,领导者产生区块并递交给所有其他节点对区块进行验证,进而其他节点“举

手”表决时接受或拒绝该领导者的提议。如果大部分节点认为当前领导者存在问题,这些节点也可以通过多轮的投票协商过程将现有领导者推翻,再以某种预先定好的协议协商产生出新的领导者节点。

BFT 类算法一般都有完备的安全性证明,能在算法流程上保证在群体中恶意节点数量不超过三分之一时,诚实节点的账本保持一致。然而,这类算法的协商轮次也很多,协商的通信开销也比较大,导致这类算法普遍不适用于节点数目较大的系统。业界普遍认为,BFT 算法所能承受的最大节点数目不超过 100。

- 结合可信执行环境的共识算法

上述三类共识算法均为纯软件的共识算法。除此之外,还有一些共识算法对硬件进行了利用,如一些利用可信执行环境(Trusted Execution Environment,TEE)的软硬件结合的共识算法。

可信执行环境是一类能够保证在该类环境中执行的操作绝对安全可信、无法被外界干预修改的运行环境,它与设备上的普通操作系统(Rich OS)并存,并且能给 Rich OS 提供安全服务。可信执行环境所能够访问的软硬件资源是与 Rich OS 完全分离的,从而保证了可信执行环境的安全性。

利用可信执行环境,可以对区块链系统中参与共识的节点进行限制,很大程度上可以消除恶意节点的不规范或恶意操作,从而能够减少共识算法在设计时需要考虑的异常场景,一般来说能够大幅提升共识算法的性能。

2.2.4 智能合约

智能合约的引入可谓区块链发展的一个里程碑。区块链从最初单一数字货币应用,至今天融入各个领域,智能合约可谓不可或缺。这些金融、政务服务、供应链、游戏等各种类别的应用,几乎都是以智能合约的形式,运行在不同的区块链平台上。

1. 智能合约是什么?

其实,智能合约并不是区块链独有的概念。早在 1995 年,跨领域学者 Nick Szabo 就提出了智能合约的概念,他对智能合约的定义为:“一个智能合约是一套以数字形式定义的承诺,包括合约参与方可以在上面执行这些承诺的协议。”简单来说,智能合约是一种在满足一定条件时,就自动执行的计算机程序。例如自动售货机,就可以视为一个智能合约系统。客户需要选择商品,并完成支付,这两个条件都满足后售货机就会自动吐出货物。

合约在生活中处处可见:租赁合同、借条等。传统合约依靠法律进行背书,当产生违约及纠纷时,往往需要借助法院等政府机构的力量进行裁决。智能合约,不仅仅是将传统的合约电子化,它的真正意义在革命性地将传统合约的背书执行由法律替换成了代码。俗话说,“规则是死的,人是活的”,程序作为一种运行在计算机上的规则,同样是“死的”。但是“死的”也不总是贬义词,因为它意味着会严格执行。

比如,球赛期间的打赌即可以通过智能合约实现。首先在球赛前发布智能合约,规定:今

天凌晨 2:45,欧冠皇马 VS 拜仁慕尼黑,如果皇马赢,则小明给我 1 000 元;如果拜仁赢,我给小明 1 000 元。我和小明都将 1 000 元存入智能合约账户,比赛结果发布,皇马 4∶2 胜拜仁,触发智能合约响应条件,钱直接打入我的账户,完成履约。整个过程非常高效、简单,不需要第三方的中间人进行裁决,也完全不会有赖账等问题。

2. 为什么区块链的出现使智能合约受到了广泛的关注?

尽管智能合约这个如此前卫的理念早在 1995 年就被提出,但是一直没有引起广泛的关注。虽然这个理念很美好,但是缺少一个良好的运行智能合约的平台,确保智能合约一定会被执行,执行的逻辑没有被中途修改。区块链这种去中心化、防篡改的平台,完美地解决了这些问题。智能合约一旦在区块链上部署,所有参与节点都会严格按照既定逻辑执行。基于区块链上大部分节点都是诚实的基本原则,如果某个节点修改了智能合约逻辑,那么执行结果就无法通过其他节点的校验而不会被承认,即修改无效。

3. 智能合约的原理

一个基于区块链的智能合约需要包括事务处理机制、数据存储机制以及完备的状态机,用于接收和处理各种条件。并且事务的触发、处理及数据保存都必须在链上进行。当满足触发条件后,智能合约即会根据预设逻辑,读取相应数据并进行计算,最后将计算结果永久保存在链式结构中。智能合约在区块链中的运行逻辑如图 2.4 所示:

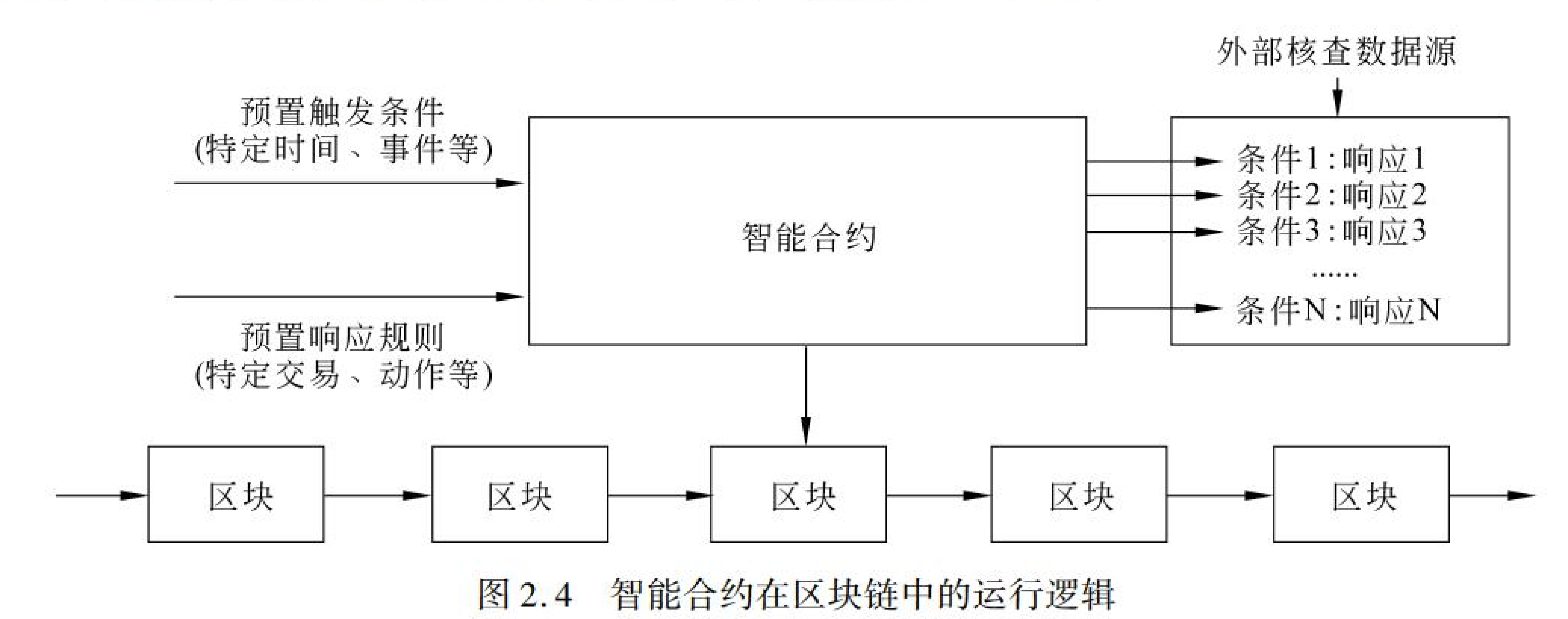


图 2.4　智能合约在区块链中的运行逻辑

对应前面打赌的例子,智能合约即为通过代码实现的打赌内容。该智能合约预置的触发条件即为规定球赛场次、时间等相关信息,同时需要规定获取结果途径(例如直接从官网获取结果)。预置响应条件即为触发事件后,智能合约具体执行内容。条件 1:皇马赢,响应 1:钱直接打入我的账户;条件 2:拜仁赢,响应 2:钱直接打入小明账户。该智能合约一经部署,其内容就会永久地保存在链上,并严格执行。球赛结束后,区块链网络中的节点均会验证响应条件,并将执行结果永久记录在链上。

4. 智能合约的安全性需要关注

因为合约是严肃的事情,传统的合约往往需要专业的律师团队来撰写。古语有云:“术

业有专攻。”当前智能合约的开发工作主要由软件从业者来完成,其所编写的智能合约在完备性上可能有所欠缺,因此相比传统合约,更容易产生逻辑上的漏洞。另外,由于现有的部分支持智能合约的区块链平台提供了利用如 Go 语言、Java 语言等高级语言编写智能合约的功能,而这类高级语言不乏一些具有“不确定性”的指令,可能会造成执行智能合约节点的某些内部状态发生分歧,从而影响整体系统的一致性。因此,智能合约的编写者需要极为谨慎,避免编写出有逻辑漏洞或是执行动作本身有不确定性的智能合约。不过,一些区块链平台引入了不少改进机制,对执行动作上的不确定性进行了消除,如超级账本项目的 Fabric 子项目,即引入了先执行、背书、验证,再排序写入账本的机制;以太坊项目也通过限制用户只能通过其提供的确定性的语言(Ethereum Solidity)进行智能合约的编写,确保了其上运行的智能合约在执行动作上的确定性。

2016 年著名的 The DAO 事件,就是因为智能合约漏洞导致大约几千万美元的直接损失。The DAO 是当时以太坊平台最大的众筹项目,上线不到一个月就筹集了超过 1 000 万个以太币,当时价值一亿多美元。但是该智能合约的转账函数存在漏洞,攻击者利用该漏洞,盗取了 360 万个以太币。由于此事件影响过大,以太坊最后选择进行回滚硬分叉挽回损失。The DAO 智能合约的具体内容感兴趣的读者可以自行查阅①。但是我们并不能因此而否认智能合约的价值,任何事物在发展初期必然因为不完善而存在风险,因噎废食并不可取。

随着智能合约的普及,智能合约的编写必然会越来越严谨、规范,同时,其开发门槛也会越来越低,对应领域的专家也可参与到智能合约的开发工作中,智能合约必定能在更多的领域发挥越来越大的作用。随着技术的发展和大家对智能合约安全的重视,从技术上可以对智能合约进行静态扫描,发现潜在问题反馈给智能合约开发人员,也可以通过智能合约形式化验证的方法全面地发现智能合约中存在的问题。

2.2.5 P2P 网络

传统的网络服务架构大部分是客户端/服务端(client/server,C/S)架构,即通过一个中心化的服务端节点,对许多个申请服务的客户端进行应答和服务。C/S 架构也称为主从式架构,其中服务端是整个网络服务的核心,客户端之间通信需要依赖服务端的协助。例如当前流行的即时通信(Instant Message,IM)应用大多采用 C/S 架构:手机端 APP 仅被作为一个客户端使用,它们之间相互间收发消息需要依赖中心服务器。也就是说,在手机客户端之间进行消息收发时,手机客户端会先将消息发给中心服务器,再由中心服务器转发给接收方手机客户端。

C/S 架构的优势非常明显且自然:单个的服务端能够保持一致的服务形式,方便对服务进行维护和升级,同时也便于管理。然而,C/S 架构也存在很多缺陷。首先,由于 C/S 架构只有单一的服务端,因此当服务节点发生故障时,整个服务都会陷入瘫痪。另外,单个服务端节

① 查阅地址:https://github.com/TheDAO/DAO-1.0.

点的处理能力是有限的，因此中心服务节点的性能往往成为整体网络的瓶颈。

对等计算机网络（Peer-to-Peer Networking，P2P 网络），是一种消除了中心化的服务节点，将所有的网络参与者视为对等者（Peer），并在他们之间进行任务和工作负载分配。P2P 结构打破了传统的 C/S 模式，去除了中心服务器，是一种依靠用户群共同维护的网络结构。由于节点间的数据传输不再依赖中心服务节点，P2P 网络具有极强的可靠性，任何单一或者少量节点故障都不会影响整个网络正常运转。同时，P2P 网络的网络容量没有上限，因为随着节点数量的增加，整个网络的资源也在同步增加。由于每个节点可以从任意（有能力的）节点处得到服务，同时由于 P2P 网络中暗含的激励机制也会尽力向其他节点提供服务，因此，实际上 P2P 网络中节点数目越多，P2P 网络提供的服务质量就越高。

P2P 网络实际是一个具有较长发展历史的技术，典型的代表性技术及发展历程如下所示。

- 最早可追溯到 1979 年杜克大学研究生 Tom Truscott 及 Jim Ellis 开发出的使用 P2P 结构的新闻聚合网络 USENET。由于当时计算机及计算机网络还处于初步发展阶段，文件的传输需要通过效率较低的电话线进行，集中式的控制管理方法效率极其低下，便催生了 P2P 网络这种分布式的网络结构。
- 随着 P2P 网络技术的发展，在 20 世纪 90 年代，出现了世界上第一个大型的 P2P 应用网络：Napster。它同样是由几位大学生进行开发，用于共享 mp3 文件。Napster 采用一个集中式的服务器提供它所有的 mp3 文件的存储位置，而将 mp3 文件本身放置于千千万万的个人电脑上。用户通过集中式的服务器查询所需 mp3 文件的位置，再通过 P2P 方式到对等节点处进行下载。Napster 由于版权问题，被众多唱片公司起诉而被迫关闭，然而其所用的 P2P 技术却因此而广为传播。
- 借鉴 Napster 的思想，Gnutella 网络于 2000 年早期被开发。这是第一个真正意义上的"分布式"P2P 网络，它为了解决 Napster 网络的中心目录服务器的瓶颈问题，采取了洪泛的文件查询方式：网络中并不存在中心目录服务器，关于 Gnutella 的所有信息都存放在分布式的节点上。用户只要安装了 Gnutella，即将自己的电脑变成了一台能够提供完整目录和文件服务的服务器，并会自动搜寻其他同类服务器。

总的来说，虽然 C/S 架构应用非常成熟，但是这种存在中心服务节点的特性，显然不符合区块链去中心化的需求。同时，在区块链系统中，要求所有节点共同维护账本数据，即每笔交易都需要发送给网络中的所有节点。如果按照传统的 C/S 这种依赖中心服务节点的模式，中心节点需要大量交易信息转发给所有节点，这几乎是不可能完成的任务。P2P 网络的这些设计思想则同区块链的理念完美契合。在区块链中，所有交易及区块的传播并不要求发送者将消息发送给所有节点。节点只需要将消息发送给一定数量的相邻节点即可，其他节点收到消息后，会按照一定的规则转发给自己的相邻节点。最终通过一传十、十传百的方式，最终将消息发送给所有节点。

以传统的银行系统为例。传统银行系统均采用 C/S 网络架构，即以银行服务器为中心节点，各个网点、ATM 为客户端。当我们需要发起转账时，首先提供银行卡、密码等信息证明身

份，然后生成一笔转账交易，发送到中心服务器后，由中心服务器校验余额是否充足等信息，然后记录到中心服务器，即可完成一笔转账交易。

而在区块链网络中，并不存在一个中心节点来校验并记录交易信息，校验和记录工作有网络中的所有节点共同完成。当一个节点需要发起转账时，需要指明转账目的地址、转账金额等信息，同时还需要对该笔交易进行签名。由于不存在中心服务器，该交易会随机发送到网络中的邻近节点，邻近节点收到交易消息后，对交易进行签名，确认身份合法性后，再校验余额是否充足等信息。均校验完成后，它则会将该消息转发至自己的邻近节点。以此重复，直至网络中所有节点均收到该交易。最后，矿工获得记账权后，则会将该交易打包至区块，然后再广播至整个网络。区块广播过程同交易的广播过程，仍然使用一传十、十传百的方式完成。收到区块的节点完成区块内容验证后，即会将该区块永久地保存在本地，即交易生效。

2.3 区块链的特性

区块链是多种已有技术的集成创新，主要用于实现多方信任和高效协同。通常，一个成熟的区块链系统具备透明可信、防篡改可追溯、隐私安全保障以及系统高可靠四大特性。

2.3.1 透明可信

1. 人人记账保证人人获取完整信息，从而实现信息透明

在去中心化的系统中，网络中的所有节点均是对等节点，大家平等地发送和接收网络中的消息。所以，系统中的每个节点都可以完整观察系统中节点的全部行为，并将观察到的这些行为在各个节点进行记录，即维护本地账本，整个系统对于每个节点都具有透明性。这与中心化的系统是不同的，中心化的系统中不同节点之间存在信息不对称的问题。中心节点通常可以接收到更多信息，而且中心节点也通常被设计为具有绝对的话语权，这使得中心节点成为一个不透明的黑盒，而其可信性也只能藉由中心化系统之外的机制来保证，如图 2.5 所示。

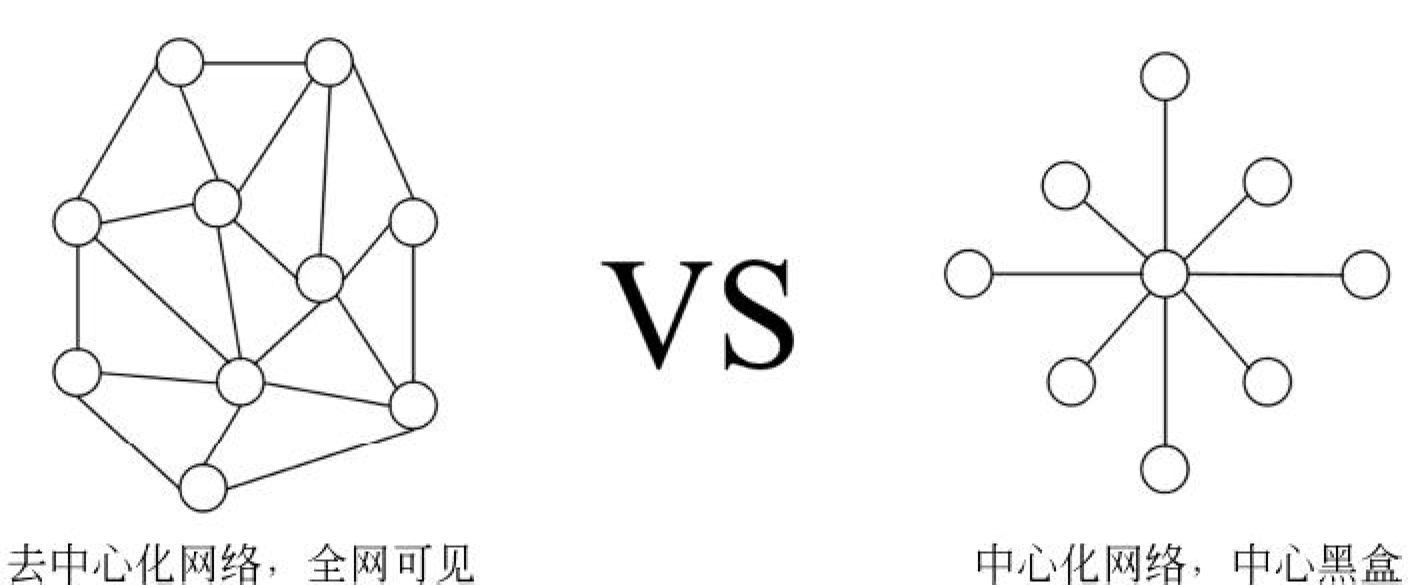


图 2.5 网络架构对比

2. 节点间决策过程共同参与，共识保证可信性

区块链系统是典型的去中心化系统，网络中的所有交易对所有节点均是透明可见的，而交易的最终确认结果也由共识算法保证了在所有节点间的一致性。所以整个系统对所有节点均是透明、公平的，系统中的信息具有可信性。

所谓共识，简单理解就是指大家都达成一致的意思。其实在现实生活中，有很多需要达成共识的场景，比如投票选举，开会讨论，多方签订一份合作协议等。而在区块链系统中，每个节点通过共识算法让自己的账本跟其他节点的账本保持一致。

2.3.2　防篡改可追溯

“防篡改”和“可追溯”可以被拆开来理解，现在很多区块链应用都利用了防篡改可追溯这一特性，使得区块链技术在物品溯源等方面得到了大量应用。

“防篡改”是指交易一旦在全网范围内经过验证并添加至区块链，就很难被修改或者抹除。一方面，当前联盟链所使用的如 PBFT 类共识算法，从设计上保证了交易一旦写入即无法被篡改；另一方面，以 PoW 作为共识算法的区块链系统的篡改难度及花费都是极大的。若要对此类系统进行篡改，攻击者需要控制全系统超过 51% 的算力，且若攻击行为一旦发生，区块链网络虽然最终会接受攻击者计算的结果，但是攻击过程仍然会被全网见证，当人们发现这套区块链系统已经被控制以后便不再会相信和使用这套系统，这套系统也就失去了价值，攻击者为购买算力而投入的大量资金便无法收回，所以一个理智的个体不会进行这种类型的攻击。

在此需要说明的是，“防篡改”并不等于不允许编辑区块链系统上记录的内容，只是整个编辑的过程被以类似“日志”的形式完整记录了下来，且这个“日志”是不能被修改的。

“可追溯”是指区块链上发生的任意一笔交易都是有完整记录的，如图 2.6 所示，我们可以针对某一状态在区块链上追查与其相关的全部历史交易。“防篡改”特性保证了写入到区块链上的交易很难被篡改，这为“可追溯”特性提供了保证。

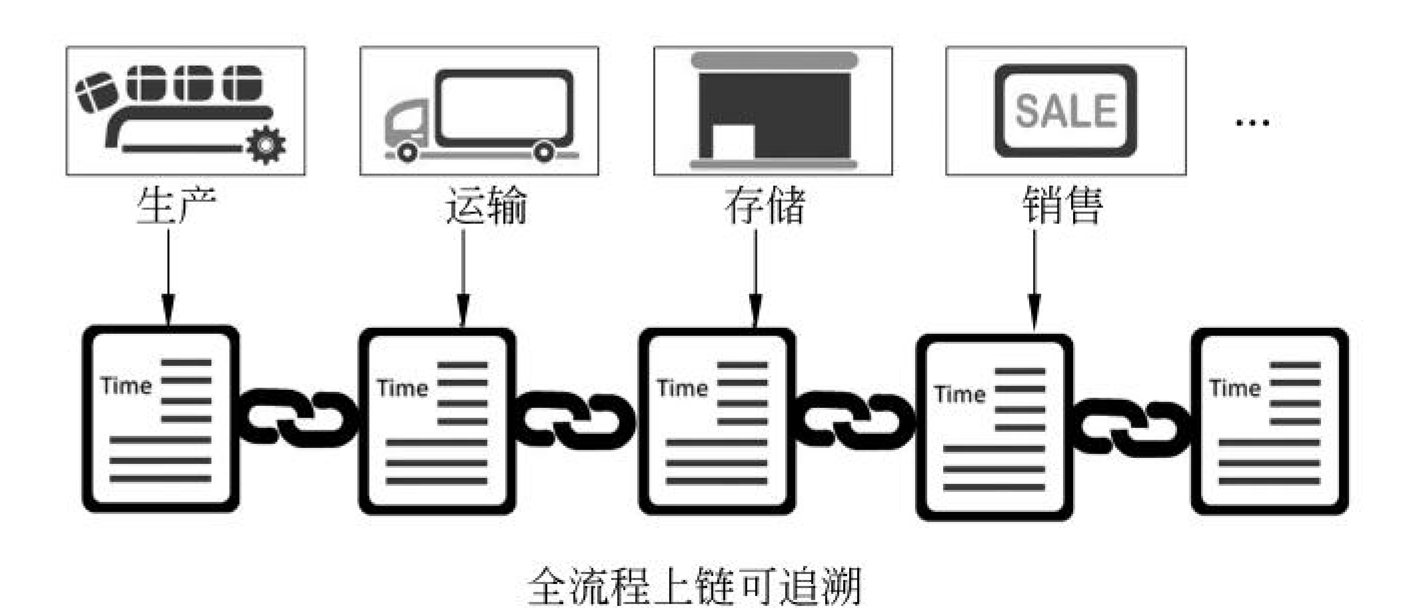
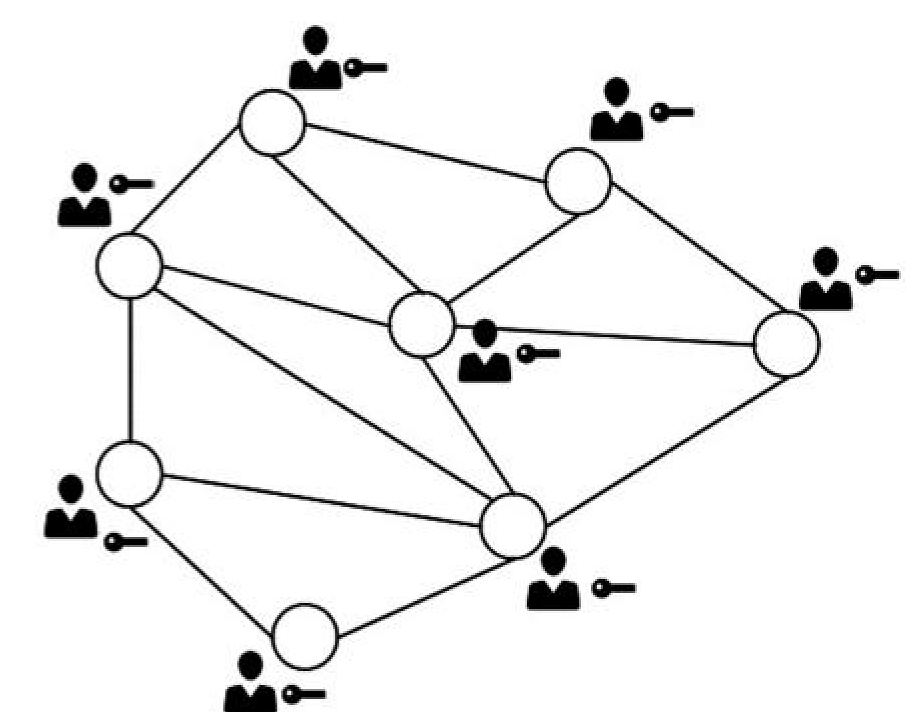


图 2.6　区块链存储信息示意图

2.3.3 隐私安全保障

区块链的去中心化特性决定了区块链的“去信任”特性：由于区块链系统中的任意节点都包含了完整的区块校验逻辑，所以任意节点都不需要依赖其他节点完成区块链中交易的确认过程，也就是无需额外地信任其他节点。“去信任”的特性使得节点之间不需要互相公开身份，因为任意节点都不需要根据其他节点的身份进行交易有效性的判断，这为区块链系统保护用户隐私提供了前提。

如图2.7所示，区块链系统中的用户通常以公私钥体系中的私钥作为唯一身份标识，用户只要拥有私钥即可参与区块链上的各类交易，至于谁持有该私钥则不是区块链所关注的事情，区块链也不会去记录这种匹配对应关系，所以区块链系统知道某个私钥的持有者在区块链上进行了哪些交易，但并不知晓这个持有者是谁，进而保护了用户隐私。



区块链各节点成员有唯一私钥

图2.7 区块链隐私保护示意图

从另一个角度来看，快速发展的密码学为区块链中用户的隐私提供了更多保护方法。同态加密、零知识证明等前沿技术可以让链上数据以加密形态存在，任何不相关的用户都无法从密文中读取到有用信息，而交易相关用户可以在设定权限范围内读取有效数据，这为用户隐私提供了更深层次的保障。

2.3.4 系统高可靠

区块链系统的高可靠体现在：(1)每个节点对等地维护一个账本并参与整个系统的共识。也就是说，如果其中某一个节点出故障了，整个系统能够正常运转，这就是为什么我们可以自由加入或者退出比特币系统网络，而整个系统依然工作正常；(2)区块链系统支持拜占庭容错。传统的分布式系统虽然也具有高可靠特性，但是通常只能容忍系统内的节点发生崩溃现象或者出现网络分区的问题，而系统一旦被攻克(甚至是只有一个节点被攻克)，或者说修改了节点的消息处理逻辑，则整个系统都将无法正常工作。

通常，按照系统能够处理的异常行为可以将分布式系统分为崩溃容错(Crash Fault Tolerance，CFT)系统和拜占庭容错(Byzantine Fault Tolerance，BFT)系统。CFT系统顾名思义，就是指可以处理系统中节点发生崩溃(crash)错误的系统，而BFT系统则是指可以处理系统中节点发生拜占庭(Byzantine)错误的系统。拜占庭错误来自著名的拜占庭将军问题，现在通常是指系统中的节点行为不可控，可能存在崩溃、拒绝发送消息、发送异常消息或者发送对自己有利的消息(即恶意造假)等行为。

传统的分布式系统是典型的CFT系统，不能处理拜占庭错误，而区块链系统则是BFT系

统,可以处理各类拜占庭错误。区块链能够处理拜占庭错误的能力源自其共识算法,而每种共识算法也有其对应的应用场景(或者说错误模型,简单来说即是拜占庭节点的能力和比例)。例如:PoW 共识算法不能容忍系统中超过 51% 的算力协同进行拜占庭行为;PBFT 共识算法则不能容忍超过总数 1/3 的节点发生拜占庭行为;Ripple 共识算法不能容忍系统中超过 1/5 的节点存在拜占庭行为等。因此,严格来说,区块链系统的可靠性也不是绝对的,只能说是在满足其错误模型要求的条件下,能够保证系统的可靠性。然而由于区块链系统中,参与节点数目通常较多,其错误模型要求完全可以被满足,所以我们一般认为,区块链系统是具有高可靠性的。

2.4　扩展阅读

2.4.1　常见哈希算法

经过前几个小节的介绍,我们已经知道,哈希算法就是把任意长度的输入变换成固定长度的输出,每个字节都会对输出值产生影响,且无法通过输出逆向计算得到输入。哈希算法主要包含构造函数及冲突解决两部分内容。

哈希算法的构造函数准则较为简单、均匀,即构造函数能够快速地计算出哈希值,同时构造函数能将关键字集合均匀地分布在输出地址集$\{0,1, \cdots, n-1\}$上,保证冲突的可能性最小。常见的构造方法包括:直接定址法、数字分析法、平方取中法、折叠法、随机数法、除留余数法等。直接定址法非常简单,通过线性函数($y = ax + b$)构造哈希值,该算法输出和输入长度相等,因此实际中很少单独使用该算法。数字分析法是取数据中某些取值较为均匀的位,丢掉分布不均匀的位,一次计算出哈希值。例如使用数字分析法计算当前员工生日的哈希时,出生年份即为丢掉的分布不均匀的数据,月份日期用来构成哈希值。平方取中法即求输入的平方,然后取中间几位作为哈希值。除上述所列,构造函数还有很多种,在此不一一介绍。当然,实际运用中的各种成熟的哈希算法库都是组合使用各种基本构造函数,从而消除哈希值输出的规律性,满足不可逆等特性。

前面已经介绍,由于输入无限而输出有限,哈希冲突(碰撞)是不可避免的,因此解决冲突是哈希法的另一个关键问题。解决冲突的方法包含开放定址法、再哈希法、链地址法等。开放定址法即在散列表中形成一个探测序列,当发生了冲突时,去寻找下一个空的散列地址,只要散列表足够大,空的散列地址总能找到。再哈希法很好理解,即产生冲突时,使用另一种算法生成下一个哈希值,该方法虽然不容易产生聚集,但是增加了计算时间。链地址法即哈希值产生冲突时,多个哈希构成一个链表。解决冲突的方法还有很多,有兴趣的读者可以自行查阅。

当前已经提出并被广泛使用的算法包括消息摘要算法(Message-Digest Algorithm, MD)系列和安全散列算法(Secure Hash Algorithm,SHA)家族。

MD 系列主要由 MIT 的 Ronald L. Rivest 设计,1989 年开发出第一个版本 MD2 算法,对输入值的字节数补齐成 16 的倍数,然后再加上一个 16 位校验值,最后基于该值输出哈希值。但是该方法如果忽略了校验将会产生冲突。为了加强算法的安全性,在 1990 年推出 MD4 版本。但是人们很快就发现了 MD4 的漏洞,利用当时的一台个人电脑几分钟就可找到 MD4 中的冲突,即发生碰撞。1991 年在 MD4 的基础上,又增加“安全—带子”(Safety-belts)的概念,推出 MD5 版本。MD5 相比 MD4 更复杂、更安全,也因此计算速度稍慢。MD5 在很长一段时间内被广泛使用,当前主流的编程语言均实现了 MD5 算法。但是,现在 MD5 也被证明不具备“强抗碰撞性”。只要通过穷举的方法,很快就可以找到一组碰撞的输入。由于计算性能的飞跃提升,当前的智能手机几秒钟就可以找到一个 hash 碰撞的例子,所以 MD5 已经不推荐作为散列方案。因此不再详细介绍 MD5 的计算过程。

SHA 家族包含 SHA-0、SHA-1、SHA-2 等,由美国国家安全局(NSA)设计,并由美国国家标准与技术研究院(NIST)发布。SHA-0 于 1993 年发布,但是发布之后很快被 NSA 撤回。1995 年发布修订版 SHA-1,修复一个在 SHA-0 中会降低杂凑安全性的缺点。SHA-0 和 SHA-1 的基本原理与 MD 算法相似。SHA-0 已经被攻破,SHA-1 目前也已经被证明不具备“强抗碰撞性”。SHA-2 又可分为 SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/224、SHA-512/256 六种不同的算法,这些算法基本结构一致,仅仅在生成的哈希值长度和循环运行次数方面存在细微的差异。

SHA-2 算法需经过补位、增加长度、取常量、迭代计算等几步操作,此处以 SHA-256 为例说明。首先将随机长度的输入值补位直到满足要求,即需要这个长度对 512 取余后的余数为 448(512 − 64)。即使输入刚好满足要求,也要进行一次补位操作。补位的规则也很简单,第一位补“1”,然后补“0”,直到长度满足要求。完成补位操作后,需再添加 64 位的长度信息,这就是为什么第一步补位是需要余数为 448。如果消息长度大于 2^{64},我们需要把长度分成 512 位的块,然后进行补位和添加长度的操作。SHA 算法在计算哈希值时,需要用到一个计算常量,在 SHA-256 中包含 64 个基础常量,这些常量是自然数中前 64 个质数的立方根的小数部分取前 32 比特而来,具体值不在此列出。在迭代计算时,SHA-2 采用 6 个基本逻辑函数,每个函数均基于 32 位字运算,同样地,这些函数的计算结果也是一个 32 位字。最终经过 64 步复杂迭代运算后,产生 256 比特的输出即为最终哈希值。

2.4.2 默克尔树

默克尔树是一种树形的数据结构,一般形态是二叉树,具有树结构的所有特点,如图 2.8 所示。默克尔树的叶子节点一般存储的是数据块,也可以是数据块的哈希值。

默克尔树的生成过程如下:将一个大数据块拆分成更多小的数据块,然后对每个数据块进行哈希运算,得到所有数据块的哈希值之后,获得一个哈希列表。接下来根据列表元素个数的奇偶特性重新再计算出哈希值,如果是偶数,则两两合并再计算哈希值,获得新的列表;如果是奇数,则前面两两计算哈希值,最后一个单独计算哈希值。重复上面的过程,最终得到

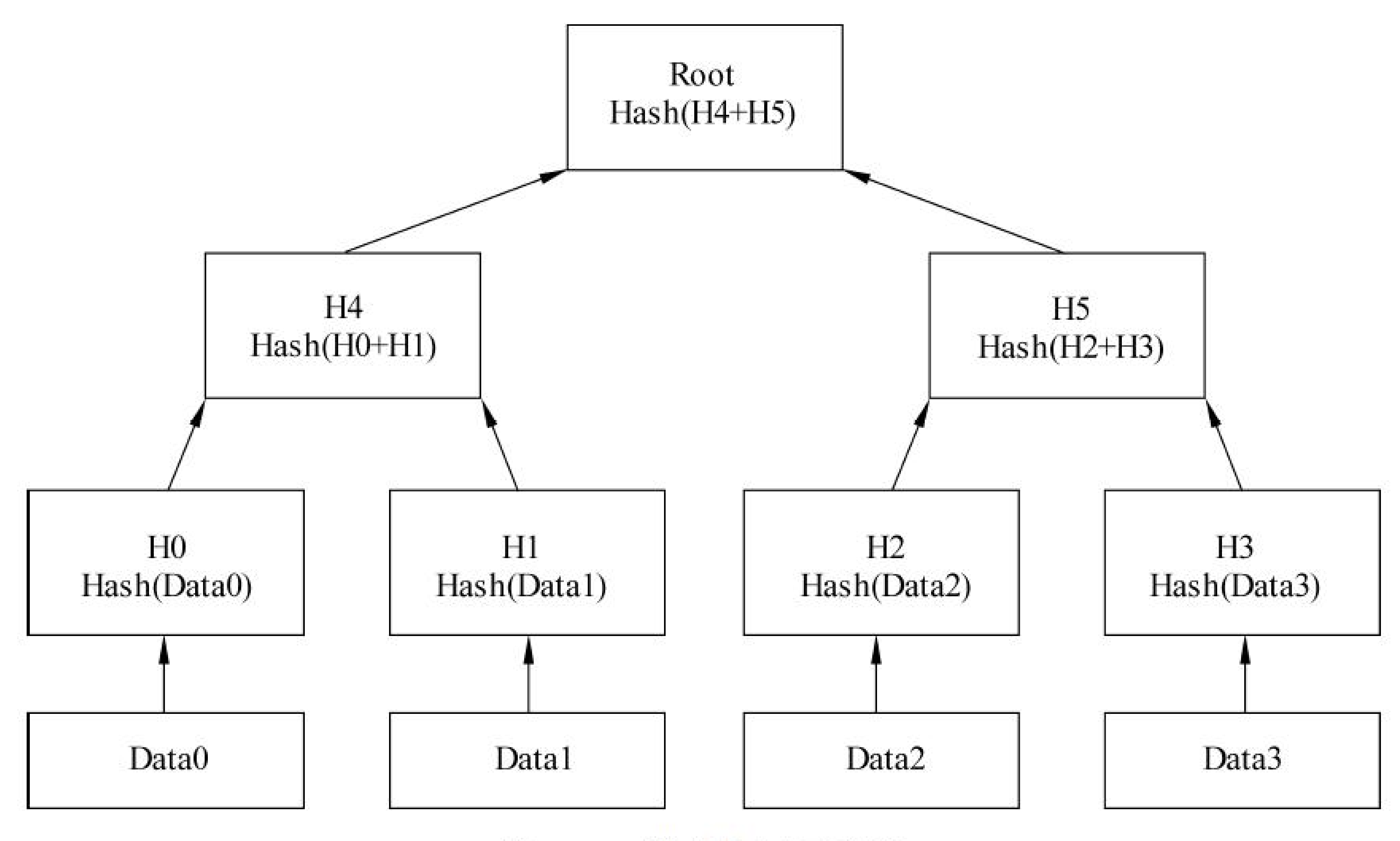


图 2.8　默克尔树示意图

一个哈希值,被称为根哈希。

默克尔树逐层记录哈希值的特点,使得它具有对数据修改敏感的特征。它有一些比较典型的应用场景。

(1) 快速比较大量数据。叶子节点数据的细微改动,都会导致根节点发生变化,可以用根节点来判断数据是否发生修改。

(2) 快速定位数据块的修改。如果 Data1 的数据发生修改,那么就会影响 H1、H4、Root。根据树的特性,从根节点到叶子节点,只需要通过 O(logn)便定位到实际发生改变的数据块是 Data1。

(3) 零知识证明。为了证明某个论断是否正确,通常我们需要将数据发送给验证者。默克尔树提供了一种方法,可以证明某方拥有某数据,而不需要将原始数据发给对方。如图 2.9 所示,我们只需要将 Data0、H1、H5、Root 对外公布,任何拥有 Data0 的用户,经过计算可以获得同样的 Root 值,说明该公开用户拥有数据 Data1、Data2、Data3。

2.4.3　常见数字签名算法

数字签名中非对称加密算法主要依赖密码学领域的单向函数原理。即正向操作非常简单,而逆向操作非常困难的函数。密码学常用的三个单项函数原理为质数分解、离散对数和椭圆曲线问题。

质数分解(prime factorization)即数学中的整数分解,将一个整数分解成几个质数的乘积。给出两个较大的质数,很快可以求得乘积。但是给定它们的乘积,无法在一定时间内分解得到两个质数。整数越大,做因数分解越困难,即满足单向函数条件。

当前流行的 RSA 算法就是采用质数分解原理。RSA 算法由 Ron Rivest、Adi Shamir 和

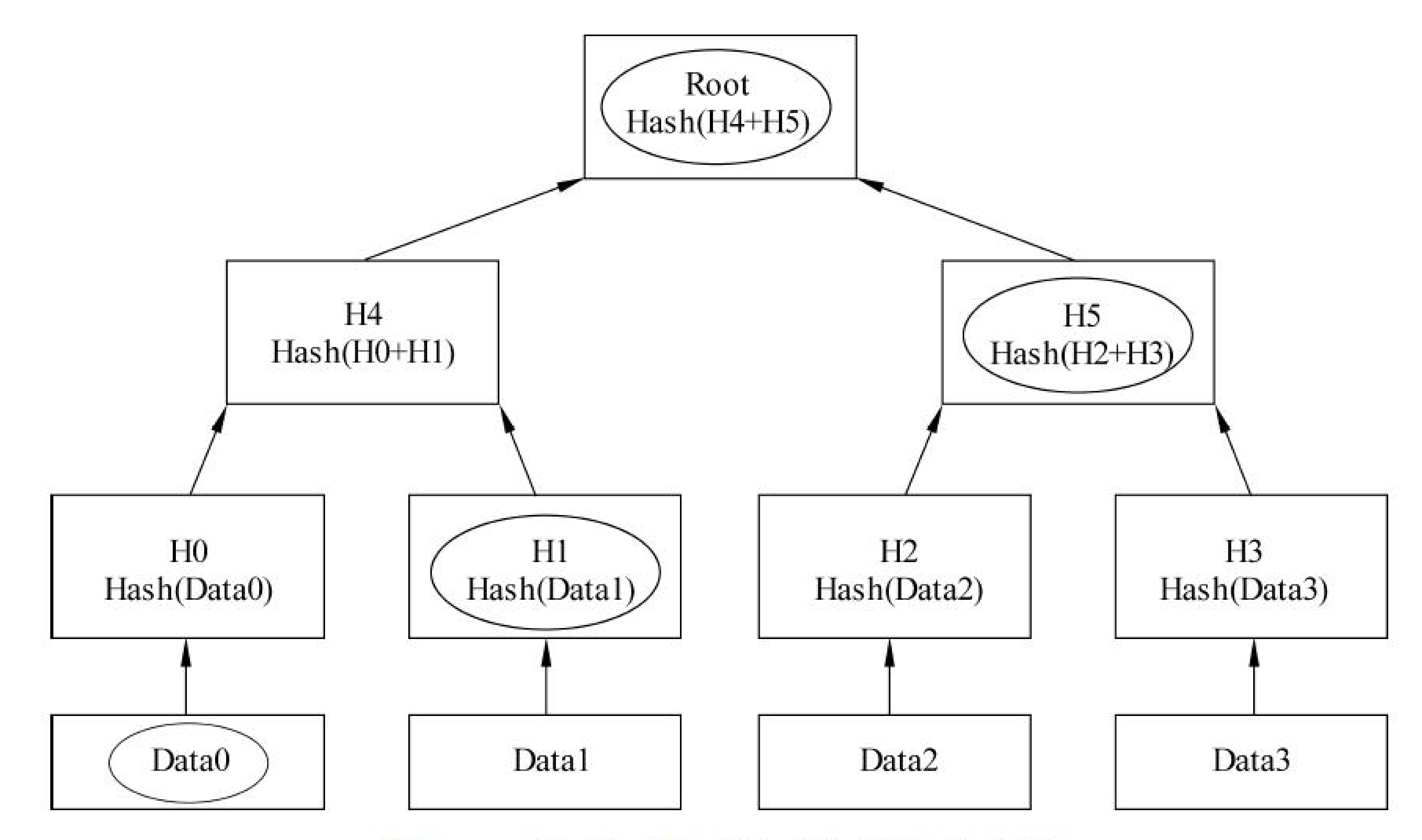


图 2.9 默克尔树在零知识证明中的应用

Leonard Adleman 于 1977 年一起提出的,RSA 就是他们三人的姓氏开头字母拼在一起组成的,三人也于 2002 年因此获得图灵奖。当前较短的 RSA 私钥可通过枚举等强力方式破解,当前应用一般推荐 2048 甚至更高长度的私钥。随着计算能力的飞速提升,特别是量子计算的发展,人们普遍认为 RSA 算法将在不久的将来被破解,所以推荐采用加密强度更高的椭圆曲线算法。

离散对数(Discrete logarithm)是一种基于同余运算和原根的一种对数运算。在实数中对数的定义 $\log_b a$ 是指对于给定的 a 和 b,有一个数 x,使得 $b^x = a$。相同地,在任何群 G 中可为所有整数 k 定义一个幂数为 b^k,而离散对数 $\log_b a$ 是指使得 $b^k = a$ 的整数 k。离散对数在一些特殊情况下可以快速计算。然而,通常没有非常高效的方法来计算它们。公钥密码学中几个重要算法的基础,是假设寻找离散对数的问题解,在仔细选择过的群中,并不存在有效率的求解算法。Diffie-Hellman 密钥交换算法是由上面提到的离散对数难题保证的。

椭圆曲线(Ellipse Curve)为一种代数曲线。其实椭圆曲线并不是我们高中学习的椭圆形状,其名字的由来是因为椭圆曲线的描述方程,类似于计算一个椭圆周长的方程。一条椭圆曲线是在射影平面上满足威尔斯特拉斯方程(Weierstrass)所有点的集合,一般形式为 $y^2 = x^3 + ax^2 + bx + c$。椭圆曲线包含两个重要特性:关于 X 轴水平对称;不垂直的直线穿过曲线最多三个点。椭圆曲线在密码学中的应用正是依赖这两个特性。

椭圆曲线算法(Ellipse Curve Cryptograph,ECC)最早于 1985 年由 Neal Koblitz 和 Victor Miller 分别独立提出,可靠性通过“椭圆曲线上的离散对数问题”的难度保证。该问题很难在短时间描述清楚,甚至可以单独写一本书介绍。即使经过 30 多年的研究,数学界仍然没有找到一个解决问题的改进办法,同样位数长度的数字,解决椭圆曲线离散对数问题要比因式分解困难得多。因此,相比 RSA,ECC 安全性能更高,160 位的 ECC 与 1024 位的 RSA 加密强度

相当。因此 ECC 的密钥长度相比 RSA 更短,存储空间更小,带宽要求更低。基于 ECC 椭圆曲线算法的数字签名算法 ECDSA,是当前主流的数字签名算法,在区块链领域应用非常广泛,比特币、Hyperledger Fabric 等区块链系统,都是采用的 ECDSA 作为数字签名算法的。

我国自主研发的 SM2 加密算法也是基于 ECC 实现。SM2 由国家密码管理局于 2010 年 12 月 17 日发布,相关标准为"GM/T 的 0003-2012《SM2 椭圆曲线公钥密码算法》"。在商用密码体系中,主要用于替换 RSA 加密算法。我国还自主研发了密码杂凑算法 SM3(类比于 SHA256 等 Hash 算法)。在金融、政务等领域,有时需要使用基于 SM2 和 SM3 的数字签名技术。

2.4.4　常见共识算法

1. 工作量证明

工作量证明(Proof of Work,PoW)是一种应对拒绝服务攻击和其他服务滥用的经济对策。它要求发起者进行一定量的运算,也就意味着需要消耗计算机一定的时间。这个概念由 Cynthia Dwork 和 Moni Naor 1993 年在学术论文中首次提出。而工作量证明(PoW)这个名词,则是在 1999 年 Markus Jakobsson 和 Ari Juels 的文章中才被真正提出。在比特币之前,哈希现金被用于垃圾邮件的过滤,也被微软用于 Hotmail/Exchange/Outlook 等产品中。工作量证明系统的主要特征是客户端需要做一定难度的工作得出一个结果,验证方却很容易通过结果来检查出客户端是不是做了相应的工作。这种方案的一个核心特征是不对称性:工作对于请求方是困难的,对于验证方则是简单的。具体来讲,每个可出块节点通过不断猜测一个数值(nonce),使得该数值拼凑上所出块中包含的交易内容的哈希值满足一定条件。由于哈希问题在目前的计算模型下是一个不可逆的问题,除了反复猜测数值,进行计算验证外,还没有有效的方法能够逆推计算出符合条件的 nonce 值。且比特币系统可以通过调整计算出的哈希值所需要满足的条件来控制计算出新区块的难度,从而调整生成一个新区块所需的时间的期望值。Nonce 值计算的难度保证了在一定的时间内,整个比特币系统中只能出现少数合法提案。另外,在节点生成一个合法提案后,会将提案在网络中进行广播,收到的用户在对该提案进行验证后,会基于它所认为的最长链的基础上继续生成下一个分叉。这种机制保证了系统中虽然可能会出现分叉,但最终会有一条链成为最长的链,被绝大多数节点所共识。

然而,由于比特币采用 SHA-256 算法,挖矿速度与机器算力成正比,这就催生了专门的"挖矿专用集成电路",即矿机。矿机的挖矿效率相比普通的 GPU 高数个数量级,带来的影响即是算力越发集中于专用矿场,使得普通用户难以入场,降低了区块链的"去中心化"程度。针对这个问题,莱特币采用了一种"内存难题算法"——Scrypt 作为其挖矿算法,其求解速度主要取决于计算机内存大小,这大大降低了大规模矿场在莱特币中的优势,使得去中心化这一特性得以保证。当前,以太坊所采用的 PoW 算法——Ethash 也与 Scrypt 类似,是一种"内存难题算法",其所要解决的主要问题也是专用矿机相比普通 PC 在挖矿上展现出来的巨大优势。

2. 权益证明

PoW 虽然是目前区块链平台采用最多的共识算法,且其可靠性已经得到了大量验证,然而 PoW 并不是没有缺陷,相反,其对能源的大量消耗一直饱受诟病,同时矿池引起的中心化问题也一直争议不断。在这样的背景下,权益证明(Proof of Stake,PoS)共识算法应运而生。最早出现的权益证明共识算法的应用是在点点币(PeerCoin,PPC)平台,这里 PoS 是一个根据你持有货币的量和时间,给你发利息的一种制度。具体地,平台里有一个名词叫币龄,每个币每天产生 1 币龄,比如你持有 100 个币,总共持有了 30 天,那么,此时你的币龄就为 3 000,这个时候,如果你发现了一个区块,你的币龄就会被清空为 0。假如你每被清空 365 币龄,将会从区块中获得 0.05 个币的利息,那么在这个案例中,利息为: $3\ 000 \times 5\% / 365 = 0.41$ 个币。在该 PoS 体系中,仍然需要挖矿,该机制只是根据币龄降低挖矿难度,加快寻找随机数的时间,这一定程度上减少了计算哈希的资源消耗。

另外一种 PoS 的实现,则是像以太坊未来会采用的共识算法一样,每个节点通过缴纳一定数量的以太币作为保证金来参与验证工作,如果权益人做出不诚实的行为,其保证金则会被罚掉。此外,Algorand、Quroboros 等都是目前很热门的 PoS 类共识算法。

3. 委托股权证明

PoS 共识算法确实可以解决很多 PoW 共识算法的问题,但是对于没币的人而言,他们并无代价可付,使得一些恶意行为对于他们是有益的,这就会导致著名的公地悲剧。在 PoS 作为共识算法的区块链系统里,上述问题叫做无利益攻击,所以必须有对付这种攻击的有效办法,否则就不能直接使用。

PoS 的一个变种算法 DPoS,就是解决无利益攻击的一种有效方式,即只有公认具有较大权益的节点才能参加共识。因此,DPoS 的本质实际上是一个中心化的共识机制。其中,EOS 网络即对 DPoS 共识算法进行了可靠尝试。

EOS 网络在刚发布的时候采用了 DPoS 的共识机制——委托股权证明(Delegated Proof of Stake,DPoS),这种共识机制的基本原理是,网络中的所有节点依据他们所拥有的代币的量,分配对应的投票权重;网络中的所有节点进行投票,选出一定数量的(EOS 使用的是 21 个)区块生产者进行新区块的生产与协商。区块生产者通过某种方式(随机或顺序)进行出块,且每个区块生产者通过出块来对之前的块进行确认。一个交易在 2/3 以上(14 个)的见证人确认后,达到不可逆状态。这样,EOS 每个超级节点在 6 秒钟之内出 12 个块,平均每半秒出一个块的速度下,一个交易需要达到不可逆状态所需的确认时间为 90 秒(需要等待 14 个其他见证人出块以确认自己)。总的来说,每期选举出固定数目的区块生产者后,区块生产者之间可建立直接连接从而保证通信的可靠及快速,DPoS 就能在较快的时间里达成共识。

4. 瑞波共识

严格来说,瑞波网络并不能算是去中心化的数字货币。在瑞波网络中,用户发起的交易经过追踪节点(tracking node)或验证节点(validating node)的广播而传递到整个网络中。其

中,追踪节点主要负责与客户端的交易请求交互及分发交易信息,验证节点则除了具有追踪节点的功能外,还负责在节点间达成并维系共识,并向账本中添加新的交易信息。

瑞波网络中的每个验证节点都预先配置了一份可信任节点名单(Unique Node List,UNL),并与名单中的每个节点维护着点对点的网络连接,因此可以实现较快的通信。每间隔一段时间,瑞波网络将进行如下的共识过程。

1）每个验证节点会不断收到从网络发送过来的交易,通过与本地账本数据验证后,不合法的交易直接丢弃,合法的交易将汇总成交易候选集(candidate set)。交易候选集里面还包括之前共识过程无法确认而遗留下来的交易。

2）每个验证节点把自己的交易候选集作为提案发送给其他验证节点。

3）验证节点在收到其他节点发来的提案后,如果不是来自 UNL 上的节点,则忽略该提案;如果是来自 UNL 上的节点,就会对比提案中的交易和本地的交易候选集,如果有相同的交易,该交易就获得一票。在一定时间内,当交易获得超过 50% 的票数时,则该交易进入下一轮。没有超过 50% 的交易,将留待下一次共识过程去确认。

4）验证节点把超过 50% 票数的交易作为提案发给其他节点,同时提高所需票数的阈值到 60%,重复步骤 3)、步骤 4),直到阈值达到 80%。

5）验证节点把经过 80% UNL 节点确认的交易正式写入本地的账本数据中,称为最后关闭账本(Last Closed Ledger),即账本最后(最新)的状态。

可以看到,在瑞波网络的共识算法中,参与共识的验证节点是事先知道的,且验证节点间的通信是很快的,因此其达成共识的效率很高,且没有 PoW 类共识算法的额外计算开销。当然,这也使得瑞波网络只适用于联盟链的场景。瑞波网络的共识拜占庭容错能力为(n－1)/5,即可以容忍验证节点的 20% 出现拜占庭错误。

5. 拜占庭将军共识

拜占庭将军问题是用来解释异步系统中存在恶意节点情况下的共识问题的一个虚构模型。拜占庭地域宽广,守卫边境的多个将军需要通过信使来传递消息,进而达成一致决定——是否攻击某一支敌军。问题是这些将军在地理上是分隔开来的,并且将军中存在叛徒。叛徒可以任意行动以达到以下目标:欺骗某些将军采取进攻;促成一个不是所有将军都同意的决定,例如,当将军们不希望进攻时促成进攻行动;或者迷惑某些将军,使他们无法做出决定。如果叛徒达到了这些目的的任意一个,则任何攻击行动都是注定要失败的,只有完全达成一致的努力才能获得胜利。拜占庭假设是对现实世界的模型化,由于硬件错误、网络拥塞或断开以及遭到恶意攻击,计算机和网络可能出现不可预料的行为。拜占庭容错协议必须处理这些失效,并且这些协议还要满足所要解决的问题要求的规范。这些算法通常以其弹性 t 作为特征,t 表示算法可以应付的错误节点数。很多经典算法问题只有在 t 小于 $n/3$ 时才有解,如实用拜占庭容错算法(PBFT),其中 n 是系统中的节点总数。

算法核心的关键在于少数人服从多数人这个策略。以 4 个将军为例,当叛变者小于或等于 1 时,系统总能达成共识。具体说明如下:将军 A 将信息传递给将军 B、C、D,且传递一定有结

果,消息简单分为进攻、撤退(分别用 0,1 表示)两种,假定大家各自的决定是进攻(0)。第一种情况,当发令者将军 A 不是叛徒,而传递后的将军中有一个叛徒(例如 B),则会有以下情况:A 的信息正确传递到 BCD,B 将错误的信息发送给 CD,但是由于 CD 发送的结果是正确的,所以最终每个节点都以多数 0 胜过了少数 1,达成一致的进攻决议。共识过程如图 2.10 所示:

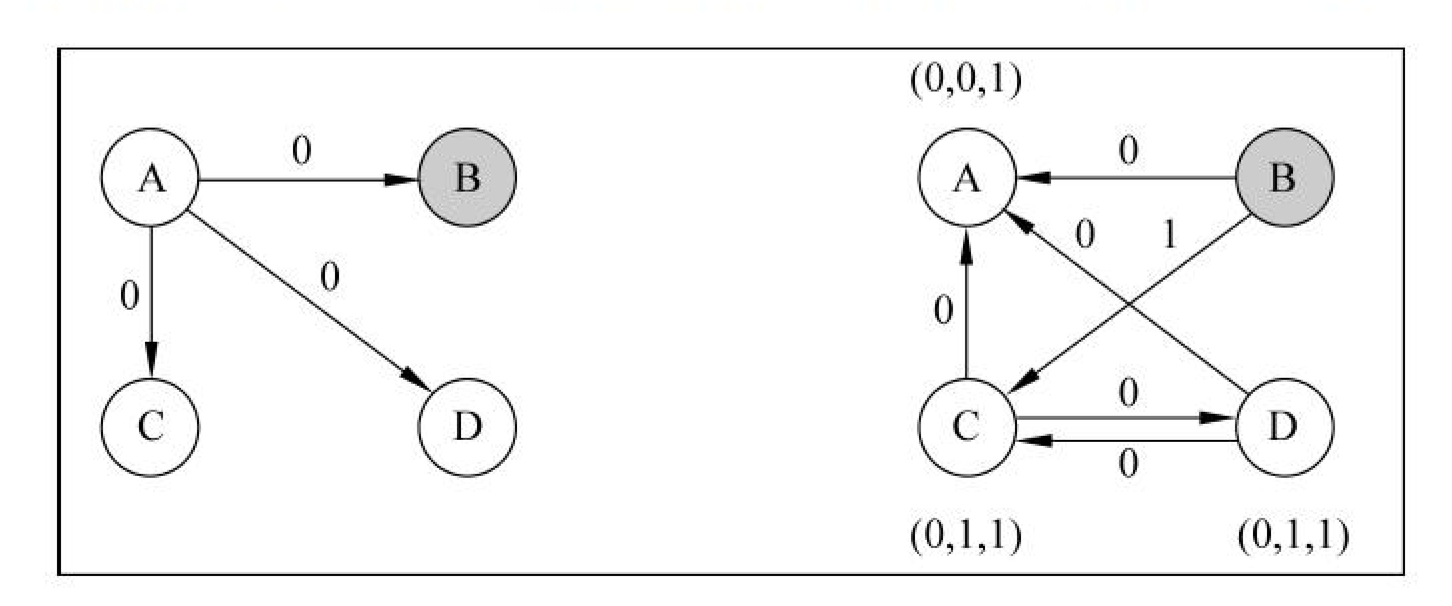


图 2.10 拜占庭将军问题提案者不是叛徒共识过程

当发令者将军 A 是叛徒时,A 向 B 发送消息 0,向 CD 发送 1。但由于 B 接收到 CD 的消息为 1,且相互传递后有四条正确信息。因此,最终结果还是以多数正确(4 个 1)赢过少数错误(2 个 0)而最终实现一致。共识过程示意图如图 2.11 所示:

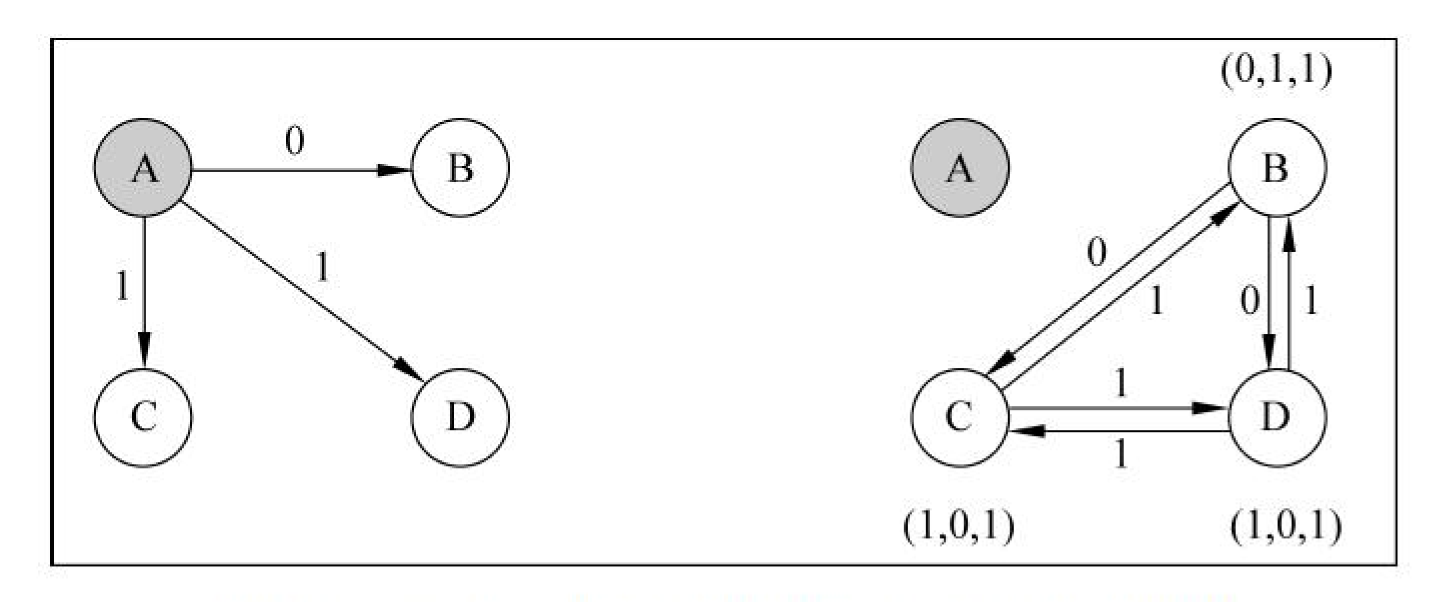


图 2.11 拜占庭将军问题提案者是叛徒共识过程

由此可见,无论哪种情形,系统均可达成一致共识。当然上述描述只是一个简单示意,具体一个完全可用的拜占庭容错共识算法可以参见 PBFT 及其变种算法,而近期大红大紫的 Algorand,其本质上也是一种拜占庭容错算法。

广义来讲,区块链系统中的共识算法均为拜占庭容错共识算法,因为区块链主要应对的就是各类外在欺骗、攻击行为,只不过前面所述的共识算法并不是强一致的共识算法,而是一种最终一致的共识算法,需要依赖链式结构或者 DAG 结构来完成算法的一致性;而如 PBFT 这样的共识算法则是强一致的共识算法,一旦经过共识便是一致确定的结果,不会出现反复的情况,这也是前述共识算法与其他类区块链共识算法的核心区别。

2.4.5 P2P 技术及常见 P2P 网络协议

目前,P2P 技术广泛应用于计算机网络的各个领域,如分布式计算、文件共享、流媒体直

播与点播、语音即时通讯、在线游戏支撑平台等。

1. 分布式计算

P2P 技术可以应用于分布式计算领域,将众多终端主机的空闲计算资源进行联合,从而服务于同一个计算量巨大的科学计算。每次计算过程中,计算任务被划分为多个片,被分配到参与计算的 P2P 节点机器上。节点机器利用闲置计算力完成计算任务,返回给一些服务器进行结果整合以达到最终结果。世界上最著名的 P2P 分布式科学计算系统非“SETI@ home”莫属,它召集具有空闲计算资源的用户组成一个分布式计算网络,共同完成通过分析射电望远镜传来的数据来搜寻地外文明的任务。

2. 文件共享

P2P 技术最直接的应用就是文件共享。在这些基于 P2P 的应用中,每个用户都可以上传文件至网络中,供其他用户下载,不需要借助中心服务器存储这些文件。用户下载完成后,也可以作为服务端,供更多用户下载。整个网络中下载人数越多,则下载速度越快。完全不会发生传统中心架构网络中,下载数量过多,导致资源抢占,速度过慢的问题。目前国内最为流行的 P2P 文件共享方案即是比特洪流。除此之外,还有不少各具特性的文件共享协议,如 Gnutella、Chord、Pastry 等。

3. 流媒体直播

P2P 模式应用于流媒体直播也是十分合适的,目前已有许多这方面的研究。目前较为成熟的流媒体直播解决方案有香港科技大学的 Coolstreaming、清华大学的 Gridmedia 等。同时,国内也涌现了很多成功的 P2P 流媒体直播商业产品,如 PPLive、PPStream 等。

4. IP 层语音通信

IP 层语音通信(Voice over Internet Protocol,VoIP)是一种全新的网络电话通信业务,它和传统的公共交换电话网(Public Switched Telephone Network,PSTN)电话业务相比,有着扩展性好、部署方便、价格低廉等明显的优点。目前,最为流行的 P2P VoIP 应用是 Skype,它能够提供清晰的语音和免费的服务,使用起来极其方便快捷。

P2P 网络技术经过几十年的发展,为适用各种不同类型的应用,催生了大量具有不同特性的网络协议,如比特币及以太坊分别采用的 Gossip、Kademlia 协议。

1. Gossip 协议

Gossip 协议由 1987 年 ACM 上发表的论文 *Epidemic Algorithms for Replicated Database Maintenance* 提出,主要应用于分布式数据库系统中各个 slave 节点的数据同步,从而保证各个节点数据的最终一致性。

Gossip 算法又被称作“病毒传播算法”、“流言算法”。这些别名可谓形象地描述了 Gossip 的工作原理。Gossip 来源于流行病学的研究,类似于病毒传播或者办公室八卦信息的传播过程,一个节点发生状态变化后,开始向邻近节点发送消息,节点收到消息后又会发送给相邻节

点，最终所有节点都会收到消息。

Gossip 协议共有 Anti-Entropy（反熵）、Rumor monge（谣言传播）两种交互模式，两种模式的介绍及相应优缺点如下：

Anti-Entropy：每个节点周期性地随机选取一定数量的相邻节点，互相同步自己的数据。该方式可以保证数据的最终一致性。但是，由于在该模式下，节点会不断地交换数据，导致网络中消息数量巨大、网络开销巨大。

Rumor monge：当一个节点收到消息后，该节点周期性地向相邻节点发送新收到的消息。由于在该模式中，节点仅在收到新消息后的一段时间内转播新消息，所以相对于 Anti-Entropy 模式来说，网络开销小很多，但是有一定概率无法达到强一致性。

实际上，在 Gossip 协议中，节点之间的同步率和节点间的通信开销是一组互相矛盾的指标。在实际应用中，需要对这一对指标进行细致的考量，即根据应用对节点同步率的具体需求和可用的网络情况作出权衡。

在 Gossip 协议中，每个节点都会维护数据的键（key）、值（value）、版本（version）信息。信息交换共支持 pull、push、pull/push 三种通信方式。例如，A、B 两个节点同步信息，三种方式的过程分别如下。

- pull：A 点将 key、version 信息发送给 B，B 收到消息后返回本地更新比 A 新的信息。
- push：A 点将 key、value、version 信息发送给 B，B 收到消息后更新比本地信息新的内容。
- pull/push：在 pull 的基础上多了一步，A 收到返回后，会再次将本地新的消息发送给 B。

2. Kademlia 协议

Kademlia 协议于 2002 年发布，是由 Petar 和 David 为非集中式 P2P 计算机网络设计的一种通过分布式散列表实现的 P2P 协议。在 Kademlia 网络中，所有信息均以哈希表条目形式加以存储，这些条目被分散地存储在各个节点上，从而在全网中构成一张巨大的分布式哈希表，在不需要服务器的情况下，每个客户端负责一个小范围的路由，并存储一小部分数据，从而实现整个分布式散列表网络的寻址和存储。Kademila 协议中使用的分布式散列表，与其他的分布式散列表技术相比，具有以异或算法（XOR）为距离度量基础的特性，大大提高了路由查询速度。

Kademlia 协议也对节点间的信息交换方式进行了规定。具体来说，Kademlia 网络节点之间使用 UDP 进行通讯。参与通讯的所有节点形成一张虚拟网（或者叫作覆盖网），这些节点通过一组数字（或称为节点 ID）来进行身份标识。节点 ID 不仅可以用来做身份标识，还可以用来进行值定位（这里的值通常是文件的 Hash 值或者关键词）。例如，节点 ID 与文件 Hash 值直接对应，进而表示某个节点存储着能够获取对应文件和资源的相关信息。当节点作为客户端在网络中搜索某些值对应的节点（即搜索存储文件 Hash 或关键词的节点）的时候，Kademlia 算法需要知道与这些值相关的键，然后分步在网络中开始搜索。其中，每一步都会找到一些节点，这些节点的 ID 与键逐步接近，在找到对应键值（ID）的节点或者无法继续寻找

更为接近的键值时,搜索便会停止。这种搜索值的方法是非常高效的：在一个包含 n 个节点的系统的值的搜索中,Kademlia 仅访问 $O(\log(n))$ 个节点,降低了值的查询开销。

2.5　本章小结

本章主要介绍了区块链的基础技术和特性。从区块链的数据结构展开,介绍区块数据结构。详细阐述区块链中用到的哈希运算、默克尔树、数字签名、共识算法、智能合约及 P2P 网络等技术,以及这些技术实现区块链透明可信、防篡改、可追溯、隐私安全保障、系统高可靠等特性的原理。同时为满足部分读者更深层次了解区块链技术的需求,增加扩展阅读部分,详细介绍各基础技术涉及的算法原理。

如果时光倒流 10 年,那时的中本聪在想什么呢？虽然不能穿越,但从他后来的工作和若隐若现的表述中,我们大致能还原他的思路。他要把数据做成一个生命体,数据可以随着时间轴演变。为了这个目的,他做了如下假设：(1)数据是交互的;(2)数据有身份;(3)数据是连续的;(4)数据有历史,历史不可改变;(5)当下的数据正在进入历史。假使把上述 5 条中的“数据”替换成“生命”,同样成立,只是从“虚拟”进入“现实”。要实现这 5 条假设,他需要一些工具。幸运的是,这些工具大多数已经成型,但从来没有人把它们放到一块儿。

(1) 交互：交互分两层,底层是网络通讯框架,属于基础设施,早年的 bittorrent 里已经有成熟的 P2P 方案,可以直接借用;上层是人与人之间的协作,可以看作游戏,游戏需要规则,规则最大,规则就是代码化的智能合同。所以,交互需要两个技术：“P2P”和“智能合同”。

(2) 身份：身份是一个证明“我是我”的过程。网络都是虚拟的,靠谱的只有数字。一组独特的数字对应一个真实的身份。这组数字要让别人知道,又不可以被冒充。看似是个无解的难题,其实密码学早有研究,非对称加密就是为这个问题而生,公私钥配对,一个留给自己,一个送给别人。由此构建的“数字签名”恰好证明了“我就是我”。

(3) 连续：在数据流里表述连续是个难题,必须转化成前后两个实体的传承关系。实体的颗粒度不能过细,太小的不可标识;也不能过粗,太大的难以传播。因此,区块链的核心结构呼之而出：块(block)。块是时间轴上截取的一段数据流,包装一下,加上摘要。每个快记录上一个块的摘要,表明先后顺序。摘要是块的唯一标识。摘要在技术上也有成熟的办法：“哈希函数”。

(4) 历史：在第三条中,引进了哈希函数定义连续性,同时也让历史有了某种不可更改性。在工程实现上,哈希函数可以层层堆积,能够提高算法效率。“堆积”的方法是：“默克尔树”。

(5) 当下进入历史：正在发生的事,哪些能成为可以铭记的历史？这是区块链里最难的地方。历史不是它真的发生了,而是大多数人同意它发生了。转化成技术词汇,叫“共识”。在一个分布式的环境中,形成共识如同希腊城邦的超级泛民主大会,难,非常难。因此,不断有新的“共识协议”出来,相应协议解决某种相应特殊的场景,“共识协议”是正在发展的热门技术。

第 3 章

区块链与加密数字货币的关系

3.1 “链”与“币”的关系

每当提到区块链的时候,很多人会将其等同于比特币。虽然区块链技术源自比特币,甚至“区块链”的命名也是来自比特币,但区块链和比特币并不能混为一谈。

从区块链应用发展历程看,区块链技术源于比特币,类似发动机技术源于汽车,但其也可应用于轮船、火车等;比特币是区块链的成功应用,区块链是比特币的底层技术和基础架构。比特币及模仿它基于区块链技术开发的其他加密数字货币,只是区块链的第一阶段应用,并不意味着区块链只能应用在比特币或加密数字货币上。

2013 年底,Vitalik Buterin 发表以太坊(Ethereum)白皮书,将“智能合约”的概念引入区块链技术中,这标志着区块链技术应用场景已不再局限于加密数字货币领域。智能合约使得区块链实现了图灵完备(Turing Complete)——可基于区块链开发适用于任何场景的应用程序。包含智能合约等技术的区块链被称为第二代区块链。目前区块链的应用场景已扩展至金融、供应链、政务服务、物联网、社交、共享经济等领域,由此可见,加密数字货币只是区块链的应用场景之一,区块链应用场景不仅局限于加密数字货币,二者属于包含关系。

区块链按照访问和管理权限可以分为公有链(Public Blockchain)、联盟链(Consortium Blockchain)和私有链(Private Blockchain)。公有链是完全开放的区块链,全世界的人都可以参与系统维护工作,而联盟链或私有链则是有限个群体或者组织参与的区块链。“币”在不同

的区块链系统的作用和必要性不同,“币”只是公有链经济生态和模型中的一部分,区块链技术并不一定要有“币”。

公有链离开“币”的概念难以存活,这是由于公有链的开发、维护和节点的建设、运行,都需要社会大众的参与和付出,如果没有“币”作为激励,他们参加的动力从哪里来?另外,公有链对“币”的依赖也部分源自于其共识算法。通常,公有链共识算法的核心思想都是通过经济激励来鼓励节点对系统的贡献和付出,通过经济惩罚来阻止节点作恶,这种激励和惩罚的载体便是“币”。没有基于“币”的、合理的经济模型,就没有人愿意参与到公链的开发及维护中来。联盟链和私有链则与此完全不同。联盟链或私有链的参与节点的投资和收益都是较为特殊的,参与者希望从链上获得可信数据或共同完成某种业务,所以他们更有义务和责任去维护区块链系统的稳定运行。因此,PBFT 及其变种算法成为这种场景下的共识算法首选,这样,系统中一般也就不会出现“币”的概念。

从区块链技术的发展演进来看,区块链是多种技术的集成,包括智能合约、共识算法、对等网络、账本数据存储、安全隐私保护等,其本身也在不断进行技术创新。而比特币只是区块链多种技术整合的一种形式,比如,比特币提供的脚本非常简单,该脚本的表达能力非图灵完备;比特币采用工作量证明(PoW)的共识算法,而工作量证明只是多种共识算法中的一种;安全隐私保护方面,比特币通过简单的地址匿名实现对隐私的保护,而区块链技术中可使用同态加密、零知识证明等方法实现更广泛、更严格的隐私保护需求。使用不同的技术组合,可以将区块链应用于不同的企业级应用中。

随着越来越多的政府和企业使用区块链技术,隐私保护的要求逐步凸显,如保护交易者身份、交易的内容(转账金额、物流追溯中的位置等)。各个记账节点需要在保护隐私、数据密文传输的存储的前提下验证交易的合法性。不同应用的隐私保护需求不尽相同,很多需求在加密数字货币中是不存在的,因此迫切需要发展区块链技术解决这些问题。另一个要考虑的技术发展需求是监管的要求,以比特币为代表的加密数字货币有躲避监管之嫌,但是现实中公司之间的商业往来都要合规、满足监管要求,这就为区块链技术带来了新的挑战。当前一些监管问题已经找到了解决方案,其他的还在继续研究开发中。在解决这些挑战的同时,区块链技术得到了长足的发展和不断的革新。

另外,资本市场对于加密数字货币的青睐为区块链的发展提供了资源和机会,而区块链的不断发展又为加密数字货币类应用提供了更加可靠的保障,这也加固了资本市场的投资信心,二者成了相辅相成的关系。

3.2　“链圈”与“币圈”之争

虽然区块链和加密数字货币并不等同,但由于其关系密切,当大家谈论其中一个时,必然会提到另一个。有些人认为区块链技术更有价值,而有些人则热衷于投资加密数字货币,由此形成了两个不同的圈子,分别被称为“链圈”和“币圈”。

“链圈”的人关注区块链技术本身，包括大量企业创新人员、技术人员、非技术出身而对其感兴趣的人等人群，他们或研究算法以提高区块链的性能，或研究区块链的应用场景以加快其落地。对他们而言，加密数字货币只是区块链最原始的应用，区块链的潜力远不止于加密数字货币。“链圈”相信区块链技术是一场革命，能够重塑未来社会的生产关系。

“币圈”的人则主要关心加密货数字币的价值，并期望能够从中牟利。“币圈”的人包括一些投资人和投资机构，也包括一些对区块链技术丝毫不了解的投机散户。“币圈”的人也有两类，一类坚信区块链的价值，并愿意对一些币种进行长期投资，这些人可能也是“链圈”的人；另一类人并不关心区块链的长期价值，只想通过交易这些加密数字货币来获取利润。

这里的“币”在英文里面可以指“coin”，也可以指“token”。这两个单词在某些场景下，尤其在“币圈”的一些人眼中，是等效的，都是指加密数字货币，人们可以在交易所对其进行买卖。但“token”对于“链圈”的人来说意义则更广泛一些。为了和“coin”在中文里做出区分，“token”会被翻译为“通证”或“代币”。“通证”一般是由智能合约生成的，它的密码学性质使得它的拥有者是唯一确定的，且只有其拥有者有权限对其声明拥有权和转让权。所以“通证”的本质是一种权益的证明，它可以作为一种虚拟资产而存在。而与此对应，“coin”的密码学性质和“token”是一样的，但不同之处在于，它通常是指区块链主链上的加密数字货币，一般用来奖励矿工对其所参与的链的贡献。

由于智能合约可以生成代币，所以任何人或机构都可以在一个支持智能合约的公有链（如以太坊）上面发行自己的代币。如果一个机构将这个代币和一个有价值的事物绑定，比如股权，并使得别人相信这个价值在未来可以增加，那么就会有许多“币圈”的人来用他们的比特币或以太币来兑换这个代币。这家机构也因此可以募集大量的比特币或以太币。这个过程非常类似于大公司上市时的首次公开募股 IPO，因此，这种融资方式被称为首次代币发行（Initial Coin Offering，ICO）。

传统的融资方式通常需要很严格的资质审批，门槛较高，而区块链技术使得融资门槛大幅度降低，小型机构也能够在全球范围内大量的融资。表面看起来这好像是传统金融业的进步，但实际上有时候会被一些人用来做非法集资。2017 年，ICO 出现了爆炸式增长，有许多 ICO 获得了非常高额的收益，这造成了巨大的泡沫，也使得区块链技术名声在一些不明内情的人心中变坏，很多人甚至直接将区块链与诈骗相关联。对于“币圈”的这种不理性行为，“链圈”人士痛心不已，因此某些“链圈”的人会对“币圈”持不屑态度，认为“币圈”人士过于急功近利、目光短浅。

“币圈”中许多人认为区块链只有在金融领域才有活力，因为“信任”对于金融领域来说是至关重要的，而区块链技术正好提高了节点间的信任效率，所以区块链技术和金融可谓是天作之合。股票和债券可以用通证来实现，而保险和期货也可以以智能合约的形式存在。相对于传统的数字化金融产品来说，这些显然极大简化了验证流程、提升了交易效率。而实际上除金融领域的应用之外，区块链在供应链、政务服务、物联网等领域都已经有大量应用。

“链圈”和“币圈”也并非泾渭分明。有许多“链圈”的人对某些加密数字货币的前景持看

好态度，也会对其进行投资。而“币圈”的人为了识别出更好的项目，也会对区块链技术进行深入的研究。本书重点讲述区块链技术本身，对于加密数字货币的投资不作任何评述。可以预见的是，随着时间的推移，人们对于区块链和加密数字货币的理解不断加深，“链圈”与“币圈”之争也将慢慢消失。

3.3　本章小结

从第1章的比特币介绍，到第2章的区块链原理简述，很多人或许会对“币”与“链”的关系产生一些迷惑或误解。本章第1节对于二者的关系及区别进行了细致的讨论，说明了区块链是加密数字货币的技术基础，加密数字货币是区块链的重要应用。由于关注的重点不同，人们自然而然地形成了两个群体，分别为“币圈”和“链圈”。本章第2节对于两个群体的关系进行了讨论，指出这两个群体既非对立、亦无高下。明确了“链”和“币”的关系，读者才能更深入地思考区块链技术的本质，以及未来的发展前景。

第 4 章

区块链发展历史及主要框架

4.1 区块链基础技术发展历程

区块链的诞生最早可以追溯到密码学和分布式计算。

1976 年,迪菲和赫尔曼发表了一篇开创性论文《密码学的新方向》(*New Directions in Cryptography*),这篇论文覆盖了现代密码学的主要研究方向,涵盖非对称加密、椭圆曲线算法、哈希等内容,首次提出公共密钥加密协议与数字签名概念,构成了现代互联网中广泛使用的加密算法体系的基石,同时这也是加密数字货币和区块链技术诞生的技术基础。

同年,哈耶克出版了《货币的非国家化》,哈耶克从经济自由主义出发,认为竞争是市场机制发挥作用的关键,而政府对货币发行权的垄断对经济的均衡造成了破坏,通过研究竞争货币制度的可行性和优越性,哈耶克提出非主权货币(货币非国家化)、竞争发行(由私营银行发行竞争性的货币,即自由货币)等概念,从理论层面引导去中心化加密数字货币技术的发展。

1977 年 4 月,罗纳德 · 李维斯特(Ron Rivest)、阿迪 · 萨莫尔(Adi Shamir)和伦纳德 · 阿德曼(Leonard Adleman)参加了犹太逾越节的聚会,喝了些酒。回到家后李维斯特怎么都睡不着,于是信手翻阅起心爱的数学书来,这时一个灵感从他脑海浮现出来,于是连夜整理自己的思路,一气呵成写出了论文 *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*,次日李维斯特将论文拿给阿德曼审阅讨论,已经做好了再一次被击破的心理准

备，但这一次阿德曼却认输了，认为这个方案应该是可行的。在此之前阿德曼已经四十多次击破李维斯特和萨莫尔的算法。按照惯例，李维斯特按姓氏字母序将三人的名字署在论文上，也就是阿德曼、李维斯特、萨莫尔。这篇论文提出了大名鼎鼎的 RSA 算法，RSA 是一种非对称加密算法，后来在数字安全领域被广泛使用，这一工作成果被认为是《密码学新方向》的延续。

1979 年，Merkle Ralf 提出了 Merkle-Tree 数据结构和相应的算法，现在被广泛应用于校验分布式网络中数据同步的正确性，对密码学和分布式计算的发展起着重要作用，这也是比特币中用来做区块同步校验的重要手段。Merkle Ralf 是《密码学新方向》的两位作者之一 Hellman 的博士生（另一位作者 Diffie 是 Hellman 的研究助理），实际上《密码学的新方向》就是 Merkle Ralf 的博士生研究方向。

1982 年，莱斯利·兰伯特（Lamport）提出拜占庭将军问题，并证明了在将军总数大于 3f，背叛者个数小于等于 f 时，忠诚的将军们可以达成一致，标志着分布式计算理论和实践正逐渐走向成熟。

同年，大卫·乔姆公布了密码学支付系统 ECash，随着密码学的发展，具有远见的加密数字货币先驱们开始尝试将其运用到货币、支付等相关领域，ECash 是加密数字货币最早的先驱之一。

1985 年，Koblitz 和 Miller 各自独立发明了著名的椭圆曲线加密算法。由于 RSA 的算法计算量大，实际落地时遇到困难，ECC 的提出极大地推动了非对称加密体系真正进入生产实践领域并发挥巨大影响。ECC 算法标志着现代密码学理论和技术开始走向更加普遍的应用。

1997 年，Adam Back 提出了 Hashcash 算法，用于解决垃圾邮件（email spam）和 DoS（Denial-of-Service）攻击问题，Hashcash 是一种 PoW 算法，后来被比特币系统采纳使用。

1998 年，华裔工程师戴伟（Wei Dai）和尼克·萨博各自独立提出加密数字货币的概念，其中戴伟的 B-Money 被公认为比特币的精神先驱，而尼克·萨博的比特黄金（Bitgold）设想基本就是比特币的雏形，以至于至今仍有人怀疑萨博就是中本聪，但被尼克·萨博本人否定了。

21 世纪初，点对点分布式网络技术飞速发展，先后诞生了 Napster、BitTorrent 等流行应用，为加密数字货币实现夯实了技术基础。

2008 年 11 月，神秘的中本聪先生发表了论文，描述了一种完全去中心化的加密数字货币——比特币，而区块链则作为其底层技术进入公众视野。经过十年发展，区块链技术正逐渐成为最有可能改变世界的技术之一。

4.2　区块链平台发展历程

区块链的发展先后经历了加密数字货币、企业应用、价值互联网三个阶段，下面将分别对这几个阶段进行简要的介绍。

4.2.1　区块链1.0：加密数字货币

2009年1月，在比特币系统论文发表两个月之后，比特币系统正式运行并开放了源码，标志着比特币网络的正式诞生。通过其构建的一个公开透明、去中心化、防篡改的账本系统，比特币开展了一场规模空前的加密数字货币实验。在区块链1.0阶段，区块链技术的应用主要聚集在加密数字货币领域，典型代表即比特币系统以及从比特币系统代码衍生出来的多种加密数字货币。

加密数字货币的“疯狂”发展吸引了人们对区块链技术的关注，对于传播区块链技术起到了很大的促进作用，人们开始尝试在比特币系统上开发加密数字货币之外的应用，比如存证、股权众筹等。但是比特币系统作为一个为加密数字货币设计的专用系统，存在如下的问题：

（1）比特币系统内置的脚本系统主要针对加密数字货币交易而专门设计，不是图灵完备的脚本，表达能力有限，因此在开发诸如存证、股权众筹等应用时，有些逻辑无法表达，而且比特币系统内部需要做大量开发，对开发人员要求高、开发难度大，因此无法进行大规模的非加密数字货币类应用的开发。

（2）比特币系统在全球范围内只能支持每秒7笔交易，交易记账后追加6个区块才能比较安全地确认交易，追加一个块大约需要10分钟，意味着大约需要1小时才能确认交易，不能满足实时性要求较高的应用的需求。

4.2.2　区块链2.0：企业应用

针对区块链1.0存在的专用系统问题，为了支持如众筹、溯源等应用，区块链2.0阶段支持用户自定义的业务逻辑，即引入了智能合约，从而使区块链的应用范围得到了极大拓展，开始在各个行业迅速落地，极大地降低了社会生产消费过程中的信任和协作成本，提高了行业内和行业间协同效率，典型的代表是2013年启动的以太坊系统。针对区块链1.0阶段存在的性能问题，以太坊系统从共识算法的角度也进行了提升。

1. 智能合约

以太坊项目为其底层的区块链账本引入了被称为智能合约的交互接口，这对区块链应用进入2.0时代发挥了巨大作用。智能合约是一种通过计算机技术实现的，旨在以数字化方式达成共识、履约、监控履约过程并验证履约结果的自动化合同，极大地扩展了区块链的功能。

从人类分工协同的角度，现代社会已经是契约社会，而契约的签订和执行往往需要付出高昂的成本。以公司合同为例，小强机器人和小明机械签订了一笔供货合同，后来小明机械违反了合同条款，导致小强机器人供货不足产生重大损失，于是小强机器人向法院提起诉讼，在历经曲折并耗费大量人力物力后终于打赢了官司。不料小明机械拒绝履行判决，小强机器人只得向法院申请强制执行，从立案、提供人证物证到强制执行，整个流程浪费了大量社会资源。

而通过智能合约，整个履约过程将变得简单、高效、低成本。小强机器人和小明机械签订了一笔供货合同，合同以智能合约的形式通过计算机程序编码实现，经过双方确认后，供货智

能合约连同预付违约金账户被安装到区块链平台上自动执行，后来小明机械违反了合同条款，导致小强机器人供货不足产生重大损失，小强机器人提供电子证据并通过平台真实性验证后触发供货智能合约的违约赔偿条款，违约赔偿条款自动将小明机械预付的违约金按照合约规定汇入小强机器人账户作为补偿。

有了智能合约系统的支持，区块链的应用范围开始从单一的货币领域扩大到涉及合约共识的其他金融领域，区块链技术首先在股票、清算、私募股权等众多金融领域崭露头角。比如，企业股权众筹一直是众多中小企业的梦想，区块链技术使之成为现实。区块链分布式账本可以取代传统的通过交易所的股票发行，这样企业就可以通过分布式自治组织协作运营，借助用户的集体行为和集体智慧获得更好的发展，在投入运营的第一天就能实现募资，而不用经历复杂的 IPO 流程，产生高额费用。

2. 性能改进

各种区块链系统采用不同的共识方法以提升区块链的性能，比如以太坊采用改进工作量证明机制将出块时间缩短到了 15 秒，从而能够满足绝大多数的应用，以太坊未来拟采用的 PoS 共识算法可进一步提升区块链的性能。

随着区块链 2.0 阶段智能合约的引入，其“开放透明”、“去中心化”及“不可篡改”的特性在其他领域逐步受到重视。各行业专业人士开始意识到，区块链的应用也许不仅局限在金融领域，还可以扩展到任何需要协同共识的领域中去。于是，在金融领域之外，区块链技术又陆续被应用到了公证、仲裁、审计、域名、物流、医疗、邮件、鉴证、投票等其他领域，应用范围逐渐扩大到各个行业。

4.2.3　区块链 3.0：价值互联网

2018 年 5 月 28 日，国家主席习近平在中国科学院发表讲话：“进入 21 世纪以来，全球科技创新进入空前密集活跃的时期，新一轮科技革命和产业变革正在重构全球创新版图、重塑全球经济结构。以人工智能、量子信息、移动通信、物联网、区块链为代表的新一代信息技术加速突破应用”表明区块链是“新一代信息技术”的一部分。

从技术的角度来看，应用 CA 认证、电子签名、数字存证、生物特征识别、分布式计算、分布式存储等技术，区块链可以实现一个去中心、防篡改、公开透明的可信计算平台，从技术上为构建可信社会提供了可能。区块链与云计算、大数据和人工智能等新兴技术交叉演进，将重构数字经济发展生态，促进价值互联网与实体经济的深度融合。

价值互联网是一个可信赖的实现各个行业协同互联，实现人和万物互联，实现劳动价值高效、智能流通的网络，主要用于解决人与人、人与物、物与物之间的共识协作、效率提升问题，将传统的依赖于人或依赖于中心的公正、调节、仲裁功能自动化，按照大家都认可的协议交给可信赖的机器来自动执行。通过对现有互联网体系进行变革，区块链技术将与 5G 网络、机器智能、物联网等技术创新一起承载着我们的智能化、可信赖梦想飞向价值互联网时代。

30 年前，万维网之父 Tim Berners-Lee 创建了万维网，给世界带来了划时代的变革。30 年

之后的今天,Berners Lee 正在打造一个名为 Solid 的项目,旨在从根本上改变当前 Web 应用的工作方式,改善隐私,让用户真正拥有数据控制权。用户可以选择如何将这些数据用于获利,从而获得公平、安全的互联网体验。而自带密码学和去中心化属性的区块链技术在分布式身份体系的构建中具备天然优势。互联网先驱们正在积极探索如何通过区块链技术解决现有 Web 协议存在的效率低下、版本变更、中心化和骨干网依赖等问题,现阶段称其必将取代 HTTP 言之过早,但当前作为万维网协议的补充却是非常有益的。

在这个即将到来的智能价值互联时代,区块链将渗透到生产生活的方方面面,充分发挥审计、监控、仲裁和价值交换的作用,确保技术创新向着让人们的生活更加美好、让世界更加美好的方向发展。

4.3 区块链分类

根据网络范围及参与节点特性,区块链可被划分为公有链、联盟链、私有链三类。这三类区块链特性对比如表 4.1 所示。这里首先对表中术语做简要的介绍。

表 4.1 区块链的类型及其特性

	公有链	联盟链	私有链
参与者	任何人自由进出	联盟成员	个体或公司内部
共识机制	PoW/PoS/DPoS 等	分布式一致性算法	分布式一致性算法
记账人	所有参与者	联盟成员协商确定	自定义
激励机制	需要	可选	可选
中心化程度	去中心化	多中心化	(多)中心化
突出特点	信用的自建立	效率和成本优化	透明和可追溯
承载能力	3~20 笔/秒	1 000~1 万笔/秒	1 000~20 万笔/秒
典型场景	加密数字货币、存证	支付、清算、公益	审计、发行

- 共识机制:在分布式系统中,共识是指各个参与节点通过共识协议达成一致的过程。
- 去中心化:是相对于中心化而言的一种成员组织方式,每个参与者高度自治,参与者之间自由连接,不依赖任何中心系统。
- 多中心:多中心化是介于去中心化和中心化之间的一种组织结构,各个参与者通过多个局部中心连接到一起。
- 激励机制:鼓励参与者参与系统维护的机制,比如比特币系统对于获得相应区块记账权的节点给予比特币奖励。

4.3.1 公有链

公有链中的“公有”就是任何人都可以参与区块链数据的维护和读取,不受任何单个中央机构的控制,数据完全开放透明。

公有链的典型案例是比特币系统。使用比特币系统,只需下载相应的客户端。创建钱包地址、转账交易、参与挖矿,这些功能都是免费开放的。比特币开创了去中心化加密数字货币的先河,并充分验证了区块链技术的可行性和安全性,比特币本质上是一个分布式账本加上一套记账协议,但比特币尚有不足,在比特币体系里只能使用比特币一种符号,很难通过扩展用户自定义信息结构来表达更多信息,比如资产、身份、股权等,从而导致扩展性不足。

为了解决比特币的扩展性问题,以太坊应运而生。以太坊通过支持一个图灵完备的智能合约语言,极大地扩展了区块链技术的应用范围。以太坊系统中也有以太币地址,当用户向合约地址发送一笔交易后,合约激活,然后根据交易请求,合约按照事先达成共识的契约自动运行。

公有链系统完全没有中心机构管理,依靠事先约定的规则来运作,并通过这些规则在不可信的网络环境中构建起可信的网络系统。通常来说,需要公众参与、需要最大限度保证数据公开透明的系统,都适合选用公有链,如数字货币系统、众筹系统等。

公有链环境中,节点数量不定,节点实际身份未知、在线与否也无法控制,甚至极有可能被一个蓄意破坏系统者控制。在这种情况下,如何保证系统可靠可信的呢?实际在大部分公有链环境下,主要通过共识算法、激励或惩罚机制、对等网络的数据同步保证最终一致性。

公有链系统存在的问题如下所示。

1. 效率问题

现有的各类 Po * 共识,如比特币的 PoW 及以太坊计划推出的 PoS,都具有的一个很严重的问题即是产生区块的效率较低。由于在公有链中,区块的传递需要时间,为了保证系统的可靠性,大多数公有链系统通过提高一个区块的产生时间来保证产生的区块能够尽可能广泛地扩散到所有节点处,从而降低系统分叉(同一时间段内多个区块同时被产生,且被先后扩散到系统的不同区域)的可能性。因此,在公有链中,区块的高生成速度与整个系统的低分叉可能性是矛盾的,必须牺牲其中的一个方面来提高另一方面的性能。同时,由于潜在的分叉情况,可能会导致一些刚生成的区块的回滚,一般来说在公有链中,每个区块都需要等待若干个基于它的后续区块的生成,才能够以可接受的概率认为该区块是安全的。比特币中的区块在有6个基于它的后续区块生成后才能被认为是足够安全的,而这大概需要一个小时,对于大多数企业应用来说根本无法接受。

2. 隐私问题

目前公有链上传输和存储的数据都是公开可见的,仅通过“地址匿名”的方式对交易双方进行一定隐私保护,相关参与方完全可以通过对交易记录进行分析从而获取某些信息。这对于某些涉及大量商业机密和利益的业务场景来说也是不可接受的。另外在现实世界的业务中,很多业务(比如银行交易)都有实名制的要求,因此在实名制的情况下当前公有链系统的隐私保护确实令人担忧。

3. 最终确定性(Finality)问题

交易的最终确定性指特定的某笔交易是否会最终被包含进区块链中。PoW 等公有链共

识算法无法提供实时确定性,即使看到交易写入区块也可能后续再被回滚,只能保证一定概率的收敛。如在比特币中,一笔交易在经过1小时后可达到的最终确定性为99.999 9%,这对现有工商业应用和法律环境来说,可用性有较大风险。

4. 激励问题

为促使参与节点提供资源,自发维护网络,公有链一般会设计激励机制,以保证系统健康运行。但在现有大多数激励机制下,需要发行类似于比特币或代币,不一定符合各个国家的监管政策。

4.3.2 联盟链

联盟链通常应用在多个互相已知身份的组织之间构建,比如多个银行之间的支付结算、多个企业之间的物流供应链管理、政府部门之间的数据共享等。因此,联盟链系统一般都需要严格的身份认证和权限管理,节点的数量在一定时间段内也是确定的,适合处理组织间需要达成共识的业务。联盟链的典型代表是 Hyperledger Fabric 系统。

联盟链的特点如下所示。

1. 效率较公有链有很大提升

联盟链参与方之间互相知道彼此在现实世界的身份,支持完整的成员服务管理机制,成员服务模块提供成员管理的框架,定义了参与者身份及验证管理规则;在一定的时间内参与方个数确定且节点数量远远小于公有链、对于要共同实现的业务在线下已经达成一致理解,因此联盟链共识算法较比特币 PoW 的共识算法约束更少,共识算法运行效率更高,如 PBFT、Raft 等,从而可以实现毫秒级确认,吞吐率有极大提升(几百到几万 TPS)。

2. 更好的安全隐私保护

数据仅在联盟成员内开放,非联盟成员无法访问联盟链内的数据;即使在同一个联盟内,不同的业务之间的数据也进行一定的隔离,比如 Hyperledger Fabric 的通道(Channel)机制将不同业务的区块链进行隔离;在1.2版本中推出的 Private Data Collection 特性支持对私有数据的加密保护。不同的厂商又做了大量的隐私保护增强,比如华为公有云的区块链服务(Blockchain Service,BCS)提供了同态加密,对交易金额信息进行保护;通过零知识证明,对交易参与方身份进行保护等。

3. 不需要代币激励

联盟链中的参与方为了共同的业务收益而共同配合,因此有各自贡献算力、存储、网络的动力,一般不需要通过额外的代币进行激励。

4.3.3 私有链

私有链与公有链是相对的概念,所谓私有就是指不对外开放,仅仅在组织内部使用。私有链是联盟链的一种特殊形态,即联盟中只有一个成员,比如企业内部的票据管理、账务审

计、供应链管理，或者政府部门内部管理系统等。私有链通常具备完善的权限管理体系，要求使用者提交身份认证。

在私有链环境中，参与方的数量和节点状态通常是确定的、可控的，且节点数目要远小于公链。私有链的特点如下所示。

1. 更加高效

私有链规模一般较小，同一个组织内已经有一定的信任机制，即不需要对付可能捣乱的坏人，可以采用一些非拜占庭容错类、对区块进行即时确认的共识算法，如 Paxos、Raft 等，因此确认时延和写入频率较公有链和联盟链都有很大的提高，甚至与中心化数据库的性能相当。

2. 更好的安全隐私保护

私有链大多在一个组织内部，因此可充分利用现有的企业信息安全防护机制，同时信息系统也是组织内部信息系统，相对联盟链来说隐私保护要求弱一些。

相比传统数据库系统，私有链的最大好处是加密审计和自证清白的能力，没有人可以轻易篡改数据，即使发生篡改也可以追溯到责任方。

4.4　代表性系统及框架

4.4.1　比特币系统

比特币系统是区块链系统的第一个典型应用，也是为比特币这个加密数字货币设计的专用系统，本书在前述章节已对其进行了较为详细的介绍，此处不再对其发展历程和原理进行赘述，而是转而对其一些特性，如 UTXO 模型、锁定脚本和解锁脚本等进行介绍。

1. 比特币 UTXO 模型

首先，比特币系统中，是没有严格意义上的“账户”概念的，取而代之，比特币系统提出了其独特的未消费的交易输出（Unspent Transaction Output，UTXO）模型，本书中简称 UTXO 模型。UTXO 是一个包含交易数据和对应的执行代码的数据结构，所有的 UTXO 条目构成了比特币的“账本”，其中每个传统意义上的“账户”的数据可以通过与它相关的 UTXO 推断出来。

在一个具有传统“账户”概念的传统支付系统中，每个用户都对应着一个账户，支付系统会对每个账户的余额进行单独地记录和管理。当系统中有用户之间发起了支付的交易，支付系统会分别对参与交易的账户的余额信息进行检查和修改。例如，A 向 B 转账 50 元，首先需要检查 A 的账户中有 50 元的余额，再从 A 的账户中扣除 50 元，并向 B 的账户中添加 50 元。可以看到，为了保证整个系统的正确性，防止双花等情况的存在，支付系统需要确保对应的业务规则得到遵守（A 的账户中至少有 50 元的余额），同时也需要保证每个交易的“事务性”，即

原子性、一致性、隔离性及持久性(ACID)。简单来说,即保证从 A 账户扣款和向 B 账户添加款项这两个动作必须同时执行、不受其他事件影响,且不会丢失。

然而,比特币系统并没有采取如此的设计,而是创新性地提出了 UTXO 的方案。UTXO 方案的核心就在于,通过交易本身来构成系统账本,而不是通过账户信息构成账本。具体地讲,在比特币的每一笔交易(TX)中,都有"交易输入"(资产来源)和"交易输出"(资产去向),且每个交易都可以有多个交易输入和多个交易输出,交易之间按照时间戳的先后顺序排列,且任何一个交易中的交易输入都是其前序的某个交易中产生的"未花费交易输出",而所有交易的最初的交易输入都来自于 coinbase 交易,即矿工得到的挖矿奖励。

我们举出一个例子来说明 UTXO 模型下的转账过程。首先,矿工 A 挖到了 12.5 枚比特币,此后,他进行了两笔交易:首先,他将自己拥有的 5 枚比特币转账给了 B;一段时间后,他又与用户 B 合资,每人各出 2.5 枚比特币付给用户 C。在 UTXO 系统中,这样的一系列操作可由三个前后依赖的 TX 完成,见表 4.2 ~4.4。

表 4.2 示例交易 1

Coinbase 交易,#1			
	来源/去向	数额	编号
交易输入		12.5	
交易输出	A 的地址(公钥)	12.5	(1)

表 4.3 示例交易 2

Coinbase 交易,#2			
	来源/去向	数额	编号
交易输入	#1(1)	12.5	
交易输出	B 的地址(公钥)	5	(1)
	A 的地址(公钥)	7.5	(2)

表 4.4 示例交易 3

Coinbase 交易,#3			
	来源/去向	数额	编号
交易输入	#2(1)	5	
	#2(2)	7.5	
交易输出	C 的地址(公钥)	5	(1)
	B 的地址(公钥)	2.5	(2)
	A 的地址(公钥)	5	(3)

表 4.2 是这一系列交易的起始交易,交易#1。可以看到,该交易无交易输入,表示来源为 coinbase,即矿工挖出一个区块的奖励,且仅有一个交易输出,对应着接受该区块奖励的矿工

的地址。这个交易就提供了一个 UTXO,即可以理解为地址 A 有了相应数额(12.5)的未消费交易输出储备,此后,可以基于该 UTXO 进行进一步的交易。

表 4.3 是举例交易中的第二个交易,在该交易中,交易来源引用了交易#1 的未使用交易输出作为交易输入,且有两笔对应该交易输入的交易输出,分别编号为 1 和 2,其中编号为 1 的交易输出指向了 B,即意味着地址 B 现有了价值 5 个比特币的 UTXO 可以在后续交易过程中引用,(相当于 A 向 B 转账了 5 个比特币)。编号为 2 的交易的交易输出指向了 A,意味着作为交易输入的交易#1 还剩余的 7.5 个比特币又(作为找零)流入了 A 的地址,即 A 后续仍可以用价值 7.5 个比特币的 UTXO 作为交易输入。

表 4.4 是示例交易过程的最后一步,即用户 A 与用户 B 合资,每人各出 2.5 枚比特币付给用户 C。在该交易中,交易输入引用了交易#2 中的两个 UTXO,分别是交易#2 中的 1 号交易输出和 2 号输出。而对应的交易输出则有三个,其中,编号为 1 的交易输出流入了 C 的地址,价值 5 个比特币,剩下的 2 号和 3 号交易相当于对 A 和 B 的找零,分别对应着 A 和 B 提供的交易输入在该交易中未使用完的部分。

从上述的例子可以看出,比特币系统中,实际上不存在明显的“账户余额”概念,每个账户都对应着某个地址,而某个地址在某个时间点所具有的“余额”,是需要通过他具有的 UTXO 的情况进行计算得出的。在比特币系统中,这种跟踪计算由比特币钱包代为负责。

基于如此设计的 UTXO 系统,比特币如何保证 UTXO 只能被对应的地址所引用为交易输入呢? 答案是比特币的脚本特性。比特币支持较为简单的交易脚本编写,用于对相应资产使用方式的规则的制定。

2. 锁定脚本与解锁脚本

比特币系统中,交易的合法性验证依赖于两类脚本:锁定脚本与解锁脚本。实际上,比特币的交易过程中,要在交易输入中提供一个用于解锁 UTXO 的脚本,这类脚本即为“解锁脚本”,是一类能够“解决”所引用的交易输出上设定的花费条件的脚本;同时,交易的输出需要指向一个用于锁定当前交易的交易输出的脚本,这类脚本即为“锁定脚本”,该脚本的意义在于,在后续的交易中,谁能够提供与该锁定脚本匹配的解锁脚本,就能够使用该脚本所锁定的 UTXO 输出。交易的验证过程中,每个节点会通过执行当前交易的解锁脚本和当前交易所引用的上一个交易的锁定脚本来对交易进行验证,当两个脚本匹配时,交易才会被验证为有效。

比特币的交易脚本是一种基于逆波兰表示法的堆栈的执行语言。逆波兰表示法(Reverse Polish Notation,RPN)是一种由波兰数学家扬·武卡谢维奇在 1920 年引入的数学表达式方式。这种表达方式的规则是,所有的操作符都置于相应的操作数之后。例如“3 + 4”这一数学表达式,常规中缀记法表达式为“3 + 4”,而用逆波兰表示法表示为“3 4 +”;常规中缀记法的表达式“(3 + 4) × 5”用逆波兰表示法为“3 4 + 5 ×”。可以看出,这种表达方法的好处在于不需要使用括号来标识操作符的优先级,首尾遍历表达式,每遇到一个操作符,即将其前方存放的对应数目的操作数取出进行计算即可。逆波兰表达式的这种特点,使其很适合用堆栈结构进行解释。堆栈为一种特殊的数据结构,可以理解为一堆数据的集合,其中维护一个“栈顶”元素,

允许两种操作,出栈和入栈,出栈为取出并在栈中删除栈顶的元素,入栈即为在栈顶放入一个项目。栈内部的维护可以有许多种原则,如最大元素在栈顶,或者最新入栈的元素在栈顶等。利用一个栈顶维护最新入栈元素的栈,很容易实现逆波兰记法的表达式解释器: 即遇到操作数则压入栈中,遇到操作符时,从栈顶取出该操作符所需数目的操作数,进行计算后再将对应结果入栈;从左至右遍历对应表达式后,栈顶所维护的值即为表达式的值。图 4.1 是逆波兰记法的脚本语言“2 3 ADD 5 EQUAL”的执行过程。

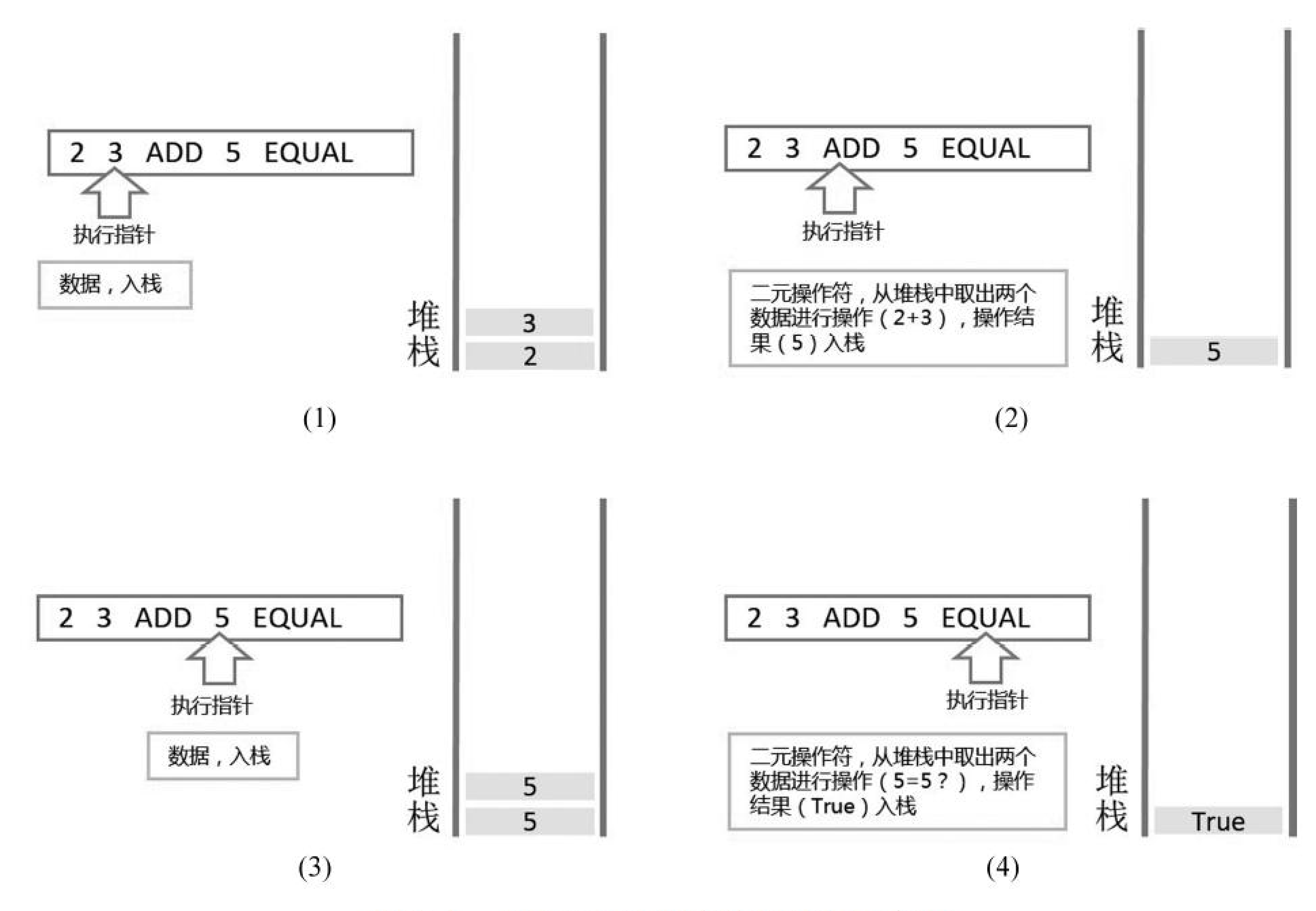


图 4.1　逆波兰记法脚本执行过程示意图

具体地讲,执行指针从命令“2 3 ADD 5 EQUAL”的头部开始执行,首先会遇到两个操作数 2 和 3,则按顺序将其压入栈中,此时堆栈中的元素由栈顶至栈底有 3,2 两个操作数;执行指针继续向右移动,遇到二元操作符“ADD”,即会从堆栈中按顺序取出两个操作数进行“ADD”操作,也就是相加操作,得到结果为 5,并将结果 5 压入堆栈中;执行指针继续右移,遇到操作数 5,即将其压入栈中,目前堆栈中的元素有 5,5 两个操作数;继续右移,遇到二元判等操作符“EQUAL”,便从堆栈中移出两个操作数,进行判等操作;判等操作结果为 True(真),即将 True 压入栈中。此时,执行指针已移至命令串末尾,执行完毕。

比特币交易脚本的语言即采用如此的执行流程,并对交易相关的一些操作符进行了规定。在编写的过程中,用户可以通过选取相应的操作符并填入相关的操作数来进行脚本的编写。

需要说明的是,比特币所使用的脚本语言,具有图灵非完备及执行结果确定这两种性质。其中,图灵非完备性对应着英国数学家图灵所提出的抽象计算模型: 确定性图灵机,它是一个

能够计算任何可计算函数的、具有无限存储能力的计算机器。若一个语言能够做到用图灵机做到的所有事情,则称该语言是“图灵完备”的。然而,由于比特币的交易脚本语言不支持循环或者较为复杂的流控制,所以它是图灵非完备的;换句话说,比特币的交易脚本的表达能力是极为有限的,其执行的流程、循环的次数都是可以预见的且确定的。然而,正是这种受限性所带来的确定性,保证了比特币的安全性。由于交易脚本语言的确定性,保证了相同的脚本在所有节点上的执行结果都是一致的,因此,一个有效的(可以通过验证的)交易在所有节点上都是有效的。相对于后期的一些支持非确定性的高级编程语言的智能合约平台,比特币在这一方面的安全性是十分可靠的。

另外,为了进一步保证比特币的安全性,比特币开发者对于客户端可以操作的脚本类型进行了限制,规定了客户端可运行的 5 种标准交易脚本,分别为 P2PKH、P2PK、P2SH、MS 和 OP_Return,对应着不同的特性和用处。接下来,我们将对这 5 类脚本进行简要的介绍。

(1) P2PKH(Pay-to-Public-Key-Hash)

该类脚本为目前比特币网络上大多数交易所采用的交易脚本。这类交易脚本包含着一个锁定脚本,对交易输出进行锁定,即公钥和对应的公钥哈希值(PKH)。比特币网络上的大多数交易都是 P2PKH 交易,此类交易都含有一个锁定脚本,该脚本由公钥哈希实现阻止输出功能,公钥哈希即广为人知的比特币地址。由 P2PKH 脚本锁定的输出可以通过键入公钥和由相应私钥创设的数字签名解锁。

下面,我们通过一个例子对 P2PKH 脚本进行介绍。假定在一笔交易中,Bob 给 Alice 支付了 0.15BTC。由于比特币并没有传统的“账户”概念,用户通过其地址(即其公钥)来标记,因此这笔交易中仅写明了 Alice 公钥的哈希值。然而,为了限定只有 Alice 才能够花费这笔交易对应的 UTXO,Bob 会在这笔 0.15BTC 的交易中创建一个输出脚本:

```
OP_DUP OP_HASH160 <Alice Public Key Hash> OP_EQUAL OP_CHECKSIG
```

这个脚本即表示对于输出交易的解锁条件,即需要提供一个签名和一个公钥。而有效的签名需要用户的私钥生成,因此仅有 Alice 能够创建出能够通过该脚本验证的签名。

Alice 在需要花费该交易中的 0.15BTC 的 UTXO 时,需要提供 Bob 生成的锁定脚本所对应的解锁脚本:

```
<Alice Signature> <Alice Public Key>
```

将解锁脚本和锁定脚本进行组合,获得如下的组合脚本:

```
<Alice Signature> <Alice Public Key> OP_DUP OP_HASH160 <AlicePublic Key Hash> OP_
EQUAL OP_CHECKSIG
```

该组合脚本的执行过程示意图如图 4.2 及 4.3 所示。

具体来说,执行指针从组合脚本的头部开始进行执行,首先遇到 <Signature> 及 <PubKey> 两个操作数,则按顺序将其压入堆栈;执行指针继续向后移动,遇到一元操作符

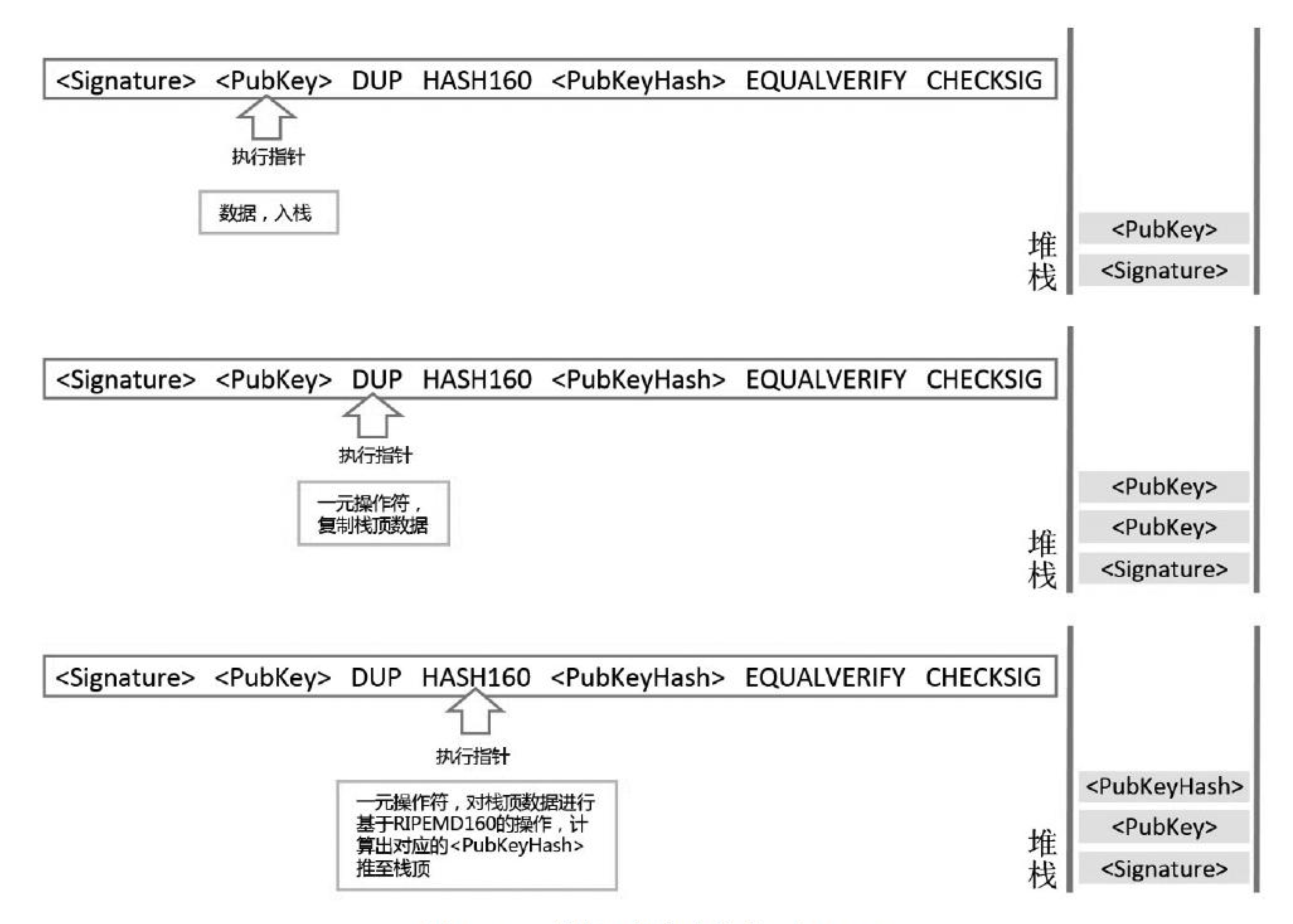


图 4.2　示例组合脚本执行过程(1)

“DUP”,该操作符的作用为复制栈顶元素并将其压入栈顶,执行完后堆栈中现有元素按从栈顶到栈底的顺序排列有：< PubKey >、< PubKey >、< Signature >三个;执行指针继续后移,遇到一元操作符“HASH160”,该操作符的作用为计算栈顶元素的哈希值,并将计算结果压入栈顶;计算完后,堆栈中现有元素的排列变成了 < PubKeyHash >、< PubKey >、< Signature >;执行指针继续后移后遇到操作数 < PubKeyHash >, 直接压入栈顶, 堆栈中元素变为 < PubKeyHash >、< PubKeyHash >、< PubKey >、< Signature >;执行指针指向的下一个操作符为二元操作符“EQUALVERIFY”,该操作符的作用为对两个操作数进行判等,若判等通过,则将两操作数移除, 并继续执行; EQUALVERIFY 成功执行完毕后, 堆栈中元素变为 < PubKey >、< Signature >,执行指针继续右移;执行指针最终指向二元操作符“CHECKSIG”,该操作符会对一组公钥和签名进行检查,确认签名是由公钥对应的私钥生成的;执行完毕后,会将对应的执行结果压入栈中。

可以看到,只有当解锁脚本与锁定脚本的设定条件相匹配时,执行组合脚本时才会显示结果为真(Ture),即只有当解锁脚本提供了 Alice 的有效签名,交易执行结果才会被通过(结果为真)。

(2) P2PK(Pay-to-Public-Key)

P2PK 模式是一种较为简单的交易脚本模式。但相比于 P2PKH,由于其并未对用户的公

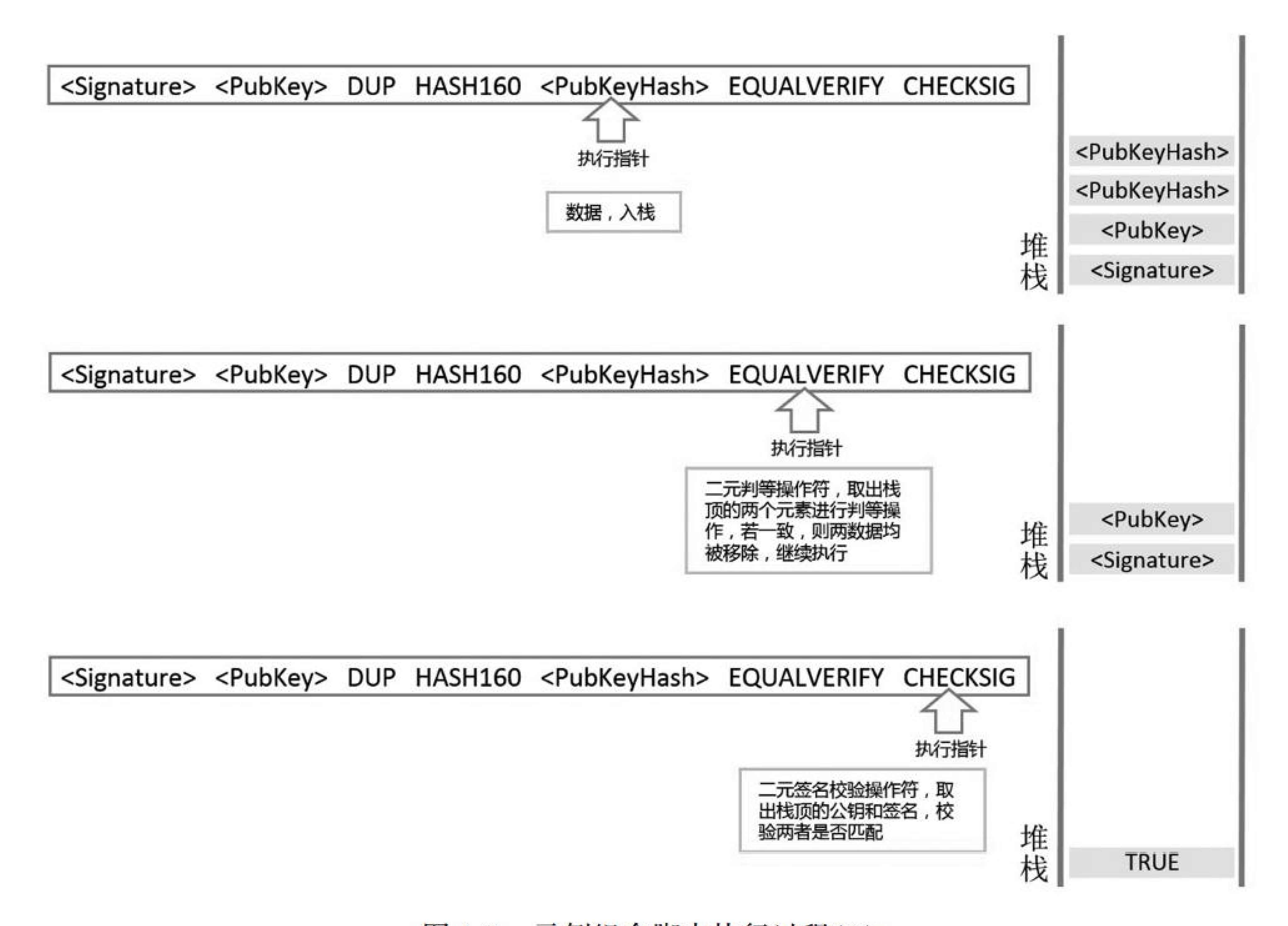


图 4.3　示例组合脚本执行过程(2)

钥进行哈希,所以可能会泄露用户公钥。目前,Coinbase 的交易常使用该模式。

在该模式中,锁定脚本的形式如下:

```
< Public Key A > OP_CHECKSIG
```

解锁脚本仅包含一个操作数,即使用者的签名:

```
< Signature from Private Key A >
```

组合脚本如下:

```
< Signature from Private Key A > < Public Key A > OP_CHECKSIG
```

该组合脚本的意义为:调用 OP_CHECKSIG 操作符,对私钥 A 的签名和私钥 A 对应的公钥进行验证,如果验证通过,则返回结果为真,通过校验。

(3) P2SH(Pay-to-Script-Hash)

P2SH 相比于前两种脚本模式具有更强的灵活性,具体说来,其仅记录 20 字节的脚本哈希,从而对具体的脚本细节进行了保护。在需要使用通过该类脚本锁定的 UTXO 时,出示对应哈希值的原始脚本,并保证脚本的运行结果为真即可。

在该模式中,锁定脚本的形式如下:

```
HASH160 PUSHDATA(目标脚本哈希) EQUAL
```

解锁时提供对应的目标脚本即可。

(4) 多重签名(Multi-Signature)

多重签名提供了这样一种解锁场景,即在相关的 N 个公钥中,需要提供 M 个公钥对应的签名,才可以对相应 UTXO 进行解锁。这类脚本在涉及多方协商交易的场景下较为有效。

在该模式中,通用的 M-N 多重签名锁定脚本(M 为至少需要提供的签名数量,N 为涉及的公钥总数)的形式如下:

```
M <Public Key 1> <Public Key 2> …<Public Key N> N OP_CHECKMULTISIG
```

对应的解锁脚本的形式如下:

```
OP_0 <Signature k> <Signature j> …
```

锁定脚本与解锁脚本结合,即可对提供的签名进行验证,从而达到多重签名锁定的目的。

(5) 数据记录输出(OP_Return)

数据记录输出脚本主要用于对比特币功能的拓展。通过该类脚本,开发者可以在交易输出上增加 80 字节的非交易数据。

比特币交易脚本可以视为是智能合约的雏形,不过它的机制相对来说比较简单,仅是一个堆栈式的指定 OP 指令解析引擎,所能够支持的规则较少,难以实现复杂的逻辑。然而比特币脚本无疑给后续区块链系统的智能合约的提出提供了一个原型,相当于给区块链系统增添了一个功能拓展接口,使区块链能够在更多的场景下发挥作用。

可以说,比特币系统作为区块链领域的开山之作,其中各种设计都是非常精巧且值得借鉴的。当前,比特币已经走过了十年,除部分交易所因为自身防范不周曾发生过被黑客盗取储备币等问题,目前还没有因为比特币自身的机制产生过严重的安全问题,同时,比特币系统的各种设计仍被各类区块链系统广为借鉴和拓展。

3. 比特币的安全性及 51%攻击

比特币的安全性保证源于其独特的 PoW 共识机制,以及其每个节点都可以独立正确验证的交易脚本机制。

要分析比特币系统的安全性,我们应首先考虑在比特币系统中可能存在的攻击形式。一个攻击者若想通过攻击比特币系统获益,显然是需要掌控“记账权”,即产生区块的权力。由于比特币系统中,由谁来产生下一个区块是一个完全随机的事件,因此,由一个攻击者节点产生部分区块是完全有可能的,但由于比特币中的正常节点都会对产生区块中的交易进行验证(通过运行交易中的锁定脚本和解锁脚本),因此,所有诚实的节点都不会接受包含了无效交易的区块,这意味着攻击者无法凭空创造价值,也无法对不属于自己的比特币进行掠夺,攻击者所能够进行的仅仅是对自己发出的交易信息进行修改(因为它无法伪造其他参与者的签名等信息)。一个典型的攻击场景即为“双花攻击”,在这种攻击中,攻击者先将自己所拥有的资

产(UTXO)在一笔交易(记为 TX1)中支付给另一个参与者以换取某些其他资产,该交易被写入当前比特币区块链(记为链 A)的第 $N+1$ 个区块;此时攻击者同时秘密地准备另一条基于原比特币区块链第 N 个区块的后续链(记为链 B),该链中并不包含 TX1;攻击者等待实际获取到 TX1 交易中所涉及的其他资产之后,再使用自己准备的这条秘密链 B 同原记录有 TX1 交易的链 A 进行替换,便可“抹消”自己所参与的 TX1 交易,收回自己在 TX1 交易中所使用的 UTXO。

当然,由于比特币的“最长链胜出”原则,攻击者秘密生成的链 B 需要在替换时比原有链 A 更长,才能够成功实行双花攻击。而比特币系统中采用的 PoW 机制保证了,某节点产生下一个区块的概率与该节点的算力占所有参与 PoW 的节点的算力的比例成正比,因此,双花攻击的成功概率与攻击节点的算力密切相关。

在实践方面,若交易双方在记录其交易 TX1 的区块 $N+1$ 生成后,等待若干个(记为 z 个)基于该区块的后续区块的成功生成之后,再对 TX1 交易进行确认(即进行交易所涉及其他资产的交接),此时攻击者若要用自己秘密生成的链 B 成功替换已生成的这 z 个区块所在的链 A(即在相同的时间内生成数量多于 z 个区块),其难度显然是与 z 的长度相关的。

我们不妨做如下的假定来对恶意节点在 z 个区块生成后仍能够成功进行攻击的概率进行分析:

$$p = \text{诚实节点制造出下一个区块的概率}$$

$$q = \text{恶意节点制造出下一个区块的概率}$$

若使用 q_z 来表示攻击者最终在 z 个区块长度时,产生的链 B 的长度超过了诚实者产生的链 A 的长度(成功攻击),则 q_z 可表示为:

$$q_z = \begin{cases} 1, & \text{若 } p < q \\ \left(\dfrac{q}{p}\right)^z, & \text{若 } p > q \end{cases}$$

可以看到,在恶意节点产生区块的概率 q 小于诚实节点产生区块的概率 p 时(亦即,恶意节点的总算力小于诚实节点的总算力时),恶意节点攻击成功的概率随着链的区块数的增长而呈指数化下降。中本聪在比特币白皮书中,对这种攻击实行的可能性进行了分析,同时给出了一系列关于 q、z,以及对应攻击成功的概率 q_z 的计算结果。

当 $q=0.1$,即恶意节点的总算力占所有节点总算力的 10% 时,对应的 z 值和 q_z 的值如表 4.5 所示。

表 4.5　恶意节点占 10% 算力时对应的 z 值和 q_z

z	0	1	2	3	4	5	6	10
q_z	100%	20.5%	5.19%	1.32%	0.346%	0.091 4%	0.024 3%	0.000 12%

当 $q=0.3$,即恶意节点的总算力占所有节点总算力的 30% 时,对应的 z 值和 q_z 的值如表 4.6 所示。

表 4.6　恶意节点占 30%算力时对应的 z 值和 q_z

z	0	5	10	15	20	25	30	50
q_z	100%	17.7%	4.17%	1.01%	0.248%	0.061 3%	0.015 2%	0.000 06%

需要说明的是，q 所代表的恶意攻击者的比例实际上应该是所有“合谋”的恶意攻击者的比例，因为它们需要互相配合以在同一条恶意链上进行延续。中本聪也给出了保证攻击成功率 $q_z < 0.1\%$ 时，z 随 q 的变化规律如表 4.7 所示。

表 4.7　保证攻击成功率小于 0.1%时 z 与 q 的变化

q	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45
z	5	8	11	15	24	41	89	340

在当前比特币系统中，由于参与计算的算力总量是十分可观的，攻击者所能够掌控的算力的总比例实际上是非常小的，因此，目前的比特币系统中，一般取 6 个区块作为交易确认时间，即在交易被写入区块后再等待 6 个基于该区块的区块的生成（一般是 60 分钟），再实际进行该交易其他资产的交接。

4. 比特币的隐私模型

传统的交易系统为交易的参与者提供了一定程度的隐私保护。具体地，用户需要将交易信息和个人身份信息递交给可信任的第三方，由可信任的第三方对用户信息和交易信息进行维护。这种方案具有一定的安全性，因为可信任的第三方通常会采取一些措施对于自己保存的用户信息和交易信息进行保密。然而，可信任的第三方也不是完全安全的，它可能会被攻击者攻破，也存在因为某些利益原因主动将部分数据交由其他人进行处理和分析的风险。

在比特币系统中，由于所有的交易都会被广播至全网，所以传统的中心化的隐私保护方法均不适用。然而，由于比特币的独特设计，用户的隐私依然可以得到保护。正如前面章节所述，比特币系统中不存在“账户”，其账本是由一个个交易组成的，而交易中的参与者仅是一系列“地址”，或者说是公钥。公众能够从公开的账本中得知的信息仅仅是某些地址将一定数量的货币发送给了另一些地址，然而，对于具体的地址与人的对应关系却一无所知。作为额外的防护措施，比特币的使用者甚至可以在每次交易中都产生并使用一个新的地址，从而使交易的追溯更加困难。从比特币被发明到现在的十年间，中本聪作为发明者和较大量的比特币持有者，其真实身份一直未被大众所获知，也可以从一定程度上说明比特币的隐私保护功能的强大。

然而需要指明的是，比特币系统虽然可以通过地址和用户不对应的方式对用户隐私进行保护，但其账本完全公开的特性，也给所有人提供了分析账本数据、找出特定地址交易规律从而定位地址与人的对应关系的可能。

4.4.2　以太坊系统

随着比特币的蓬勃发展,越来越多的人参与到比特币的交易、研究之中。由于比特币本身在当时是一个“极客”的新生事物,参与到比特币社区的人也大多都是各有抱负的年轻极客。在当时参与讨论的极客群体中,有一位出生于1994年的俄罗斯青年Vitalik Buterin(后被称为V神)。在感受到比特币的魅力之后,Vitalik决定完全投入到这样的一个完全去中心化的系统的研究之中。2013年,Vitalik高中毕业后进入以计算机科学闻名的加拿大滑铁卢大学,但倍感在学校的学习不能够完全满足他想与更多的区块链爱好者交流学习的需求,于是,在入学仅8个月后便毅然退学,走访美国、西班牙、意大利以及以色列等国家的比特币开发者社群,并积极参与到比特币转型工作之中。

然而,随着Vitalik对比特币转型工作,即寻求比特币在加密数字货币以外的应用的开展,Vitalik意识到比特币系统在设计上具有一些先天的局限性,比如带来巨大能源损失的挖矿机制,而这些局限性是难以通过后期的完善来克服的。因此,Vitalik决定自己开发出一个全新的区块链平台,该平台的目的主要在于扩展比特币区块链在更多领域的应用,将以太坊建成通用的平台,让所有的开发者都能够利用该平台,构建各种各样的去中心化应用(Decentralized Application,DApp)。以太坊改进了比特币的挖矿方式,使得大规模专用矿机不再有优势,同时为以太坊平台增添了“智能合约”的功能,即开发者能够基于以太坊虚拟机提供的智能合约开发接口,对他们自己的去中心化应用进行搭建。

Vitalik于2013年年末发表了以太坊白皮书,并于2014年1月在美国佛罗里达州迈阿密举行的北美比特币会议上,正式宣布了以太坊这个项目。同时,为了迅速地推广自己的以太坊生态,以太坊于2014年6月开始,以42天的预售活动的形式,对以太坊系统中的第一批以太币进行了分配。这次预售活动一共融资了31 591个比特币,在当时,价值大概1 800万美元,共交换出60 102 216个以太币。以当时的价格计算,相当于一个以太币0.3美元,然而截至本书成稿时,单枚以太币的价值已达到200美元的量级。

在本部分,我们将对以太坊的一些设计思路,包括其账户模型、采用的挖矿算法、提供的智能合约实现等,进行简要的介绍。

1. 以太坊账户模型

与比特币不同,以太坊没有采用UTXO模型,而是采用了传统记账系统的账户模型,即每个用户对应一个直接记录余额的账户,交易中附带有参与交易的账户的信息。相比于比特币的UTXO模型,以太坊所采用的传统账户模型显然更易于理解和进行智能合约的编程。

具体地,以太坊的每一个账户都由一对公私钥进行定义,账户的地址为其公钥的最后20个字节,以太坊通过地址来对账户进行索引。在以太坊中,共有两种账户模型:外部拥有账户(Externally owned account,EOAs)和合约账户(Contract account)。以太坊的外部拥有账户一般是给用户分配的账户,拥有该账户的用户可以通过账户对应的私钥创建和签署交易,发送消息至其他外部账户或合约账户。合约账户一般是由合约代码控制的账户,可以被外部拥有账

户触发从而执行其对应的合约代码，从而进行各种预先定义好的操作。

这些账户都是具有状态的"实体账户"（相对于比特币的"虚拟账户"），例如，外部账户有余额、合约账户有余额和合约储存。以太坊中所有账户的状态即为以太坊网络的状态，以太坊通过产生区块对其状态进行更新。

以太坊的账户状态包括如下四个部分：

（1）nonce：随机数，用于指定唯一一个交易或合约代码；

（2）balance：账户余额；

（3）root：账户状态树的树根的哈希值；

（4）codeHash：账户的合约代码的哈希值，对外部拥有账户，此字段为空；

2. 以太坊挖矿算法

以太坊采用了与比特币类似的 PoW 共识机制，但其所选用的挖矿算法却与比特币不同。在比特币所使用的 SHA-256 挖矿算法中，挖矿的速度与机器的算力成正比，从而催生了利用大规模的专用矿机的集群进行合作挖矿的集中式矿场，降低了比特币的去中心化程度，因此，以太坊采取了 Ethash 这种算法作为其工作量证明算法。Ethash 算法具有挖矿效率与内存大小和内存带宽正相关的特点，这就防止了部分矿场通过堆叠专用矿机算力而获取挖矿效率上的提升。

以太坊的挖矿算法 Ethash 又名 Dashimoto（Dagger-Hashimoto），是 Hashimoto 算法结合 Dagger 算法产生的一个变种算法。本书仅对该算法基本流程进行简要的介绍，不深入该算法的数学细节。

Ethash 算法的大致流程如下：

（1）先根据相关区块的内容计算出一个种子（seed），再利用该种子产生一定大小（例如 32MB）的伪随机数数据集，称为 cache；

（2）基于 cache，生成较大规模（1GB 以上）的数据集，称为 the DAG；DAG 中的每一个元素都是利用 cache 中的某几个元素计算得出的，并且如果给出 cache 和其中的几个指定元素，可以很快计算出 DAG 中对应的元素；

（3）挖矿的过程即为从 DAG 中随机选取元素对其进行哈希，获得一个哈希值满足指定的"难度要求"的元素。

在这种挖矿设定下，挖矿的过程需要客户端保存 DAG 的全部信息，而对挖出的区块的验证过程仅需要较小的 cache 中的信息，即验证节点仅需要基于 cache 快速计算出 DAG 中指定位置的元素，然后验证该元素的哈希值结果符合难度要求。验证过程仅需要普通 CPU 及内存即可快速完成。

在以太坊的设定中，cache 和对应的 DAG 每个周期更新一次，而一个周期的长度一般是几千个区块。因此，挖矿过程中的主要开销在于频繁地从 DAG 中读取数据进行计算，而不是对 cache 及 DAG 进行计算和更新，这即是 Ethash 算法内存敏感的原因。

以太坊的挖矿难度调整是动态进行的，每个区块的难度系数都会根据上一区块的生成时间、上一区块的难度系数以及区块高度等因素，由指定计算公式计算得出，并写在相应的区块

头中。由于以太坊尚处于不断的开发转变中,其具体使用的难度计算公式及其中的参数都处于不断的变化调整中。下面我们仅以以太坊 Homestead 阶段某时期的难度计算公式为例,对以太坊难度系数计算方法进行大致的介绍。

$$block_{diff} = parent_{diff} + \frac{parent_{diff}}{2048} \times$$
$$\max(1 - (block_{timestamp} - parent_{timestamp})/10, -99) +$$
$$int(2\hat{}((block.number/10000) - 2))$$

其中,$parent_{diff}$为上一个区块的难度系数,$block_{timestamp}$及$parent_{timestamp}$分别为该区块及上一区块产生的时间,block. number 为当前区块的序号。可以看出,当前区块的难度标准由三项组成,其中第一项是上一个区块的难度标准,第二项为根据这一个区块产生的时间计算得出的难度调整,第三项是以太坊所引入的"难度炸弹"。其中前两项主要是为了在各种算力变化下保持以太坊的出块速度维持在 15 秒左右,而第三项难度炸弹则会随着每 10 000 个区块的生成而翻倍,在后期会显著影响以太坊的出块速度。

3. 以太坊智能合约及以太坊虚拟机 EVM

以太坊为区块链系统添加了"智能合约"的实现。关于智能合约技术本身的介绍可以参考第二章中的相应章节,此处我们仅对以太坊本身所提供的智能合约进行简单的介绍。

相比于比特币所提供的极为受限的交易脚本语言,以太坊所提供的智能合约极大增强了区块链的功能,同时也为区块链赋予了可编程性。通过以太坊平台提供的智能合约编程语言和相应的对智能合约进行解释执行的以太坊虚拟机,区块链开发者可以直接在以太坊平台上进行各种可能的操作的开发,赋予以太坊区块链各种方向的应用。

我们可以将以太坊视为一个可以实现去中心化应用的平台,其核心是一套用于运行以太坊的节点所要执行的智能合约进行编程的语言,及相应地在保证节点运行其他服务的环境不受影响的条件下,对所编写的智能合约语言进行解释执行的虚拟机。用户通过调用以太坊提供的接口,对自己所希望部署的去中心化应用进行编写。在调用时,通过共识协议在所有以太坊节点间,同将要执行的智能合约达成一致,进而在每个节点的 EVM 上执行。

具体地可以将智能合约理解为代码和数据的集合。以太坊所提供的智能合约编程语言是图灵完备的,亦即以太坊的智能合约可以做到所有能够用图灵机做到的事情,类似于常见的高级编程语言,如 C ++ 、GoLang 等。以太坊提供了几套编写智能合约的高级语言,如 Solidity、Viper、Serpent 及 LLL 等,其中目前较为流行的是 Solidity 及 Viper。以太坊默认的智能合约编程语言是 Solidity,该语言编写的智能合约对应的文件扩展名为. sol,目前有许多可用的在线 Solidity 集成开发环境(IDE),如 Browser - Solidity Web IDE 等,用户可以很方便地在其上编写并编译自己所需的智能合约代码。

用户通过这些高级语言编写出较为复杂的智能合约代码后,对应的代码进而被编译为可以在 EVM 上执行的 EVM 字节码,这些字节码再被上传至以太坊区块链从而使所有节点

均可获取代码段,从而使每个节点都能够利用本地的 EVM 对字节码进行执行。EVM 在设计上具有如下的特性。

(1) 基于栈+区分存储类型:EVM 是一种基于栈的虚拟机,其对栈的大小不做限制,但限制栈调用深度为 1024;使用 256 比特的机器码,用于智能合约字节码的执行;同时,以太坊区分为临时存储和永久存储,其临时存储(Memory)存在于 EVM 的每个实例中,而其永久存储(Storage)则存在于区块链状态层。

(2) 图灵完备+Gas 限制计算量:EVM 是图灵完备的。然而,图灵完备则会导致一些问题,比如某些恶意节点可能上传无限执行的智能合约代码从而达到消耗以太坊计算资源的目的。因此,EVM 中引入了 Gas 的概念。以太坊节点在创建执行智能合约代码的消息时,需要支付一定量的 Gas 用于“购买”执行智能合约所需的计算量。当 EVM 执行交易时,Gas 将按照一定的规则逐渐被消耗,执行完后剩余的 Gas 会返还至支付节点。若在执行合约代码的过程中 Gas 被消耗殆尽,则 EVM 会触发异常,将当前已执行的相关合约代码已进行的状态修改回滚,而不会将 Gas 回退给支付节点。Gas 可以通过以太坊购买,类似于云计算中对提交任务所占用的计算资源进行付费的机制。

(3) 环境隔离:EVM 在节点上是一个隔离的环境,它保证了在其中执行的所有智能合约代码均不能影响以太坊节点中与以太坊 EVM 无关的状态,从而保证了运行 EVM 的以太坊节点的安全性。

尽管以太坊所引入的智能合约概念极大地拓展了区块链的应用范围,但其仍存在如下的一些缺陷。

(1) 缺少标准库。目前,以太坊的各类智能合约编码语言中均无高级编程语言中常见的标准库。因此,开发者进行编码的难度较高,很多开发者为了方便编程,会大段复制粘贴一些开源智能合约的实现;一方面造成了不必要的开发难度,另一方面也降低了智能合约代码的安全性(若某开源实现中的智能合约代码存在漏洞,则直接复制其部分代码的其他智能合约代码也会沿袭其漏洞);

(2) 受限的数据类型。目前,以太坊采用了极其非主流的 256bit 整数,降低了 EVM 的运算效率;同时,EVM 也不支持浮点数运算,在一定程度上限制了以太坊的应用场景;

(3) 难以调试和测试。目前 EVM 仅能抛出 OutOfGas 的异常,同时不支持调试日志的输出;同时,尽管以太坊创建了测试网络私链的功能,供开发者局部地对编写的智能合约进行测试运行,但私链对公链的模拟极其有限,使得很多智能合约代码在部署前并不能经过充分的测试,可能会引起严重的后果;

随着以太坊的不断“进阶”,以太坊社区正不断地对这些缺陷进行改善,使人们能够更方便地利用以太坊进行各类去中心化应用的开发,从而进一步扩大区块链的应用范围。

4. 典型以太坊应用

随着以太坊的不断发展,基于以太坊的开发者生态圈在目前已经相对完善。目前,已

有数千个基于以太坊开发的 DApp 正在运营中。StateoftheDApps 网站集合了当前各类 DApp(其底层平台包括但不限于以太坊)当前的用户量、交易量以及用户日活量等信息。

表4.8是StateoftheDApps 目前各平台的 DApp 数目及相关活跃信息的统计,可以看到,在目前可用的四类 DApp 开发平台中,以太坊仍占据着较大分量。

表4.8　各平台 DApp 现状统计

平台	DApp 数目	日活跃用户	日交易量	智能合约数目
以太坊	2197	29.06k	79.06k	5.25k
EOS	103	28.34k	983.7k	164
POA	13	19	1.49k	40
Steem	22	0	0	28

总的来说,目前 DApp 所涉及的领域囊括游戏、社交、赌博、金融、管理、媒体、安全、存储、能源、保险等16个领域。截至笔者定稿时,基于以太坊开发的 DApp 数目最多的四类 DApp 及其代表项目分别如下。

- 游戏类:目前有390个活跃的游戏类 DApp,包括近50%的收集类游戏如加密猫(CryptoKitties)、以太星际(0xUniverse)等,20%的模拟养成类游戏如以太小精灵、加密少女等,还有部分策略类游戏如 LORDLES、Imperial Throne 等;
- 赌博类:目前有373个活跃的赌博类 DApp,包括提供任意点到点之间的匿名赌博平台 Ninja Prediction、以太坊彩票游戏平台 Fire Lotto、扑克游戏 King Of Poker 等;
- 金融类:目前有199个活跃的金融类 DApp,包括借贷平台 MakerDAO、点到点销售平台 Dether 等;
- 社交类:目前有193个活跃的社交类 DApp,主要包括各种侧重于不同方向(如婚恋、慈善、匿名聊天等)的社交应用。

实际上,当前各类 DApp 的用户量及用户活跃度都十分有限,以太坊本身的性能无疑是限制 DApp 发展的一个重要因素。有评论认为,当前在以太坊上开发 DApp,相当于在60年代的硬件上进行计算。毕竟,以太坊交易的吞吐量、延时都远不及中心化系统,同时,在以太坊中进行信息记录的开销也十分大。

以太坊同时也提供一些基础设施服务,典型代表是以太坊域名服务(Ethereum Name Service,ENS)。ENS 是以太坊基金会开发的 DApp,它是建立在以太坊平台之上的分布式域名系统。简单来说,即是在以太坊系统中提供类似计算机网络中的域名服务(Domain Name Service,DNS)。

我们在前边的章节中提到过,以太坊的地址通常都是较长的一段无规律的字符串,难以记忆和索引(例如 ENS 的智能合约地址为0x6090A6e47849629b7245Dfa1Ca21D94cd15878Ef,十分阅读不友好且难以记忆),类似于因特网中的 IP 地址。用这类地址进行转账等操作时,很容易出现错误,也容易受到攻击(例如,用户若通过复制粘贴来输入一个转账地址,则黑客可能通

过将用户粘贴板中存储的地址调换为自己的地址,从而达到使用户错误转账给黑客的目的)。因此,ENS 旨在为部分以太网地址提供一个便于记忆的、简短易读的域名(就像 DNS 会为部分 IP 地址提供一个有意义的域名一样),在后续给对应地址进行转账时,通过直接指明对应地址的域名,即可成功进行操作。

ENS 提供的域名格式是 yourname. eth,其中 yourname 是自定义选项(需要至少八个字符),. eth 是固定项。注册 ENS 域名是一个完全去中心化的过程。通过执行 ENS 对应的智能合约,用户通过抵押一定量的以太币,参与到某一域名的拍卖之中,拍卖成功则需要把对应以太坊存在的注册合约锁定至少一年,从而获取域名的使用权。

ENS 的拍卖过程采用维克里拍卖(Vickrey auction),或称“次价密封投标拍卖”。竞拍流程主要分为三个阶段:①竞标:从域名开标到竞价截止,共计 72 个小时,此阶段接受任何人的竞标,但所有人的竞标价都会被保密;②揭标:此阶段共 48 小时,规定参加第一阶段的所有竞价者必须揭标,否则其提供抵押的 99.5% 的竞价金将被销毁;③结标:此阶段在揭标阶段之后,所有揭标者中的出价最高者以揭标者中第二高的价格获得待拍域名,投标过程中的多余款项会被退回。

至笔者截稿时,ENS 平台上已拍卖出的最贵的域名为 darkmarket,价值 20 103. 101 以太币;目前 ENS 平台已拍卖出 265 014 个域名,共发起 777 042 次拍卖,共收到 419 606 个投标,其中 275 018 次拍卖已结标。同时,随着 ENS 项目的不断发展,部分钱包应用也开始对 ENS 提供支持,其中较有代表性的是 Myetherwallet 和 Imtoken,用户可以通过 ENS 域名进行转账,同时也可以通过这两个钱包进行 ENS 域名的注册。

5. 以太坊与 ICO

尽管 V 神启动以太坊项目的初衷是为 DApp 开发者们提供开发去中心化分布式应用的平台,以太坊的大规模推广以及以太币的大幅度增值,都与 ICO 的大范围开展和 ERC-20 (Ethereum Request for Comment – 20)标准的发布息息相关。

ICO 以众筹的方式换取投资者手中的资金(通常为比特币或以太币)。而 ERC-20 标准,则是以太坊的代币设计标准,它提供了一系列基于以太坊智能合约构建的数字代币的规则和标准。利用以太坊智能合约,任何人都能够按照 ERC-20 标准中所要求的规则进行填充,编写对应的智能合约代码,从而发行自己的 ERC-20 代币,这大大降低了发行代币的门槛。

显然,比起 DApp,以太坊在数字代币发行方面的应用也很受关注。随着区块链技术的影响的扩大,在 2017 年及 2018 年年初曾掀起了一股 ICO 热潮。由于发币的成本大幅度降低,利用以太坊,甚至在 10 分钟内就可以发行一个所谓的“加密数字货币”。一时间,ICO 项目鱼龙混杂,一方面极大地提升了以太坊项目本身的影响力,另一方面又使得 ICO 项目整体的公信度急剧下降,给普通群众一种“割韭菜”的不良印象。

截至 2018 年 10 月 31 日,CoinMarketCap 网站统计了全球范围内的 2 086 个加密数字货币和 15 545 个加密数字货币交易所,全体加密数字货币的市值约 2 035 亿美元(其中比特币市值占比为 54%),过去 24 小时交易量约 106 亿美元;但 DappRadar 网站统计了以太坊及其上

的 1 137 个分布式应用，发现过去 24 小时活跃用户数只有 12 521 人，其中只有 2 个分布式应用的 24 小时活跃用户数超过或接近 1 000 人，而且比较活跃的分布式应用集中在游戏、博彩和加密资产交易等领域。

4.4.3　超级账本

超级账本(Hyperledger)是一个由 Linux 基金会牵头并创立的开源分布式账本平台，超级账本于 2015 年 12 月被正式宣布启动，由若干个各司其职的顶级项目构成。与其他区块链平台不同，Hyperledger 的各个子项目都是锚定“平台”的，仅是提供一个基于区块链的分布式账本平台，并不发币。

超级账本项目的整体目标是区块链及分布式记账系统的跨行业发展与协作，并着重发展性能和可靠性，使之可以支持主要的技术、金融和供应链公司中的全球商业交易。它的目标为开发一个“开源的分布式账本框架，构建强大的行业特定应用、平台和硬件系统，以支持商业级交易”。加入超级账本联盟的首批成员，大多是银行、金融服务公司或 IT 公司。但随着时间的推移，越来越多的公司加入了该项目。截至 2018 年 9 月 26 日的官方名单显示，有超过 270 家来自不同领域和地区的组织加入了超级账本这一项目。参与者中不乏知名巨头公司及初创公司，涉及行业从物流到医疗保健，涉及领域囊括从金融到政府组织等多个方向。截至 2018 年 7 月，超级账本拥有了 10 个子项目，涉及代码 360 万行，近 28 000 名参与者参加了超级账本的全球 110 多场相关主题聚会。

自成立以来，超级账本社区已吸引了国内外各行业的大量关注，并获得了飞速的发展。社区的各类参与者包括会员企业、开源平台开发者等，共同构造了完善的企业级区块链生态。在项目之外，超级账本开源社区的发展也极为繁荣。整体来说，社区目前的结构是“三驾马车”领导结构。

- 技术委员会(Technical Steering Committee)，负责对技术相关的工作进行领导，下设多个技术工作组，具体地对各个项目的发展进行指导。
- 管理董事会(Governing Board)，负责整体社区的组织决策，其代表座位成员从超级账本会员中推选。
- Linux 基金会(Linux Foundation)：负责基金管理和大型活动组织，协助社区在 Linux 基金会的支持下健康发展。

作为联合项目(Collaborative Project)，超级账本由面向不同目的和场景的子项目构成。目前，Hyperledger 大家庭主要包括 Burrow、Fabric、Indy、Iroha、SawTooth 5 个框架平台类的项目以及 Caliper、Cello、Composer、Explorer、Quilt 5 个工具类的项目，如图 4.4 所示。

Burrow 是最早由 Monax 开发的项目，它是一个通用的带有权限控制的智能合约执行引擎，同时也是 Hyperledger 大家庭里面第一个来源于以太坊框架的项目，智能合约引擎遵循 EVM 规范。

Fabric 是一个功能完善的支持多通道(多链)的主要面向企业应用的区块链系统，后文有

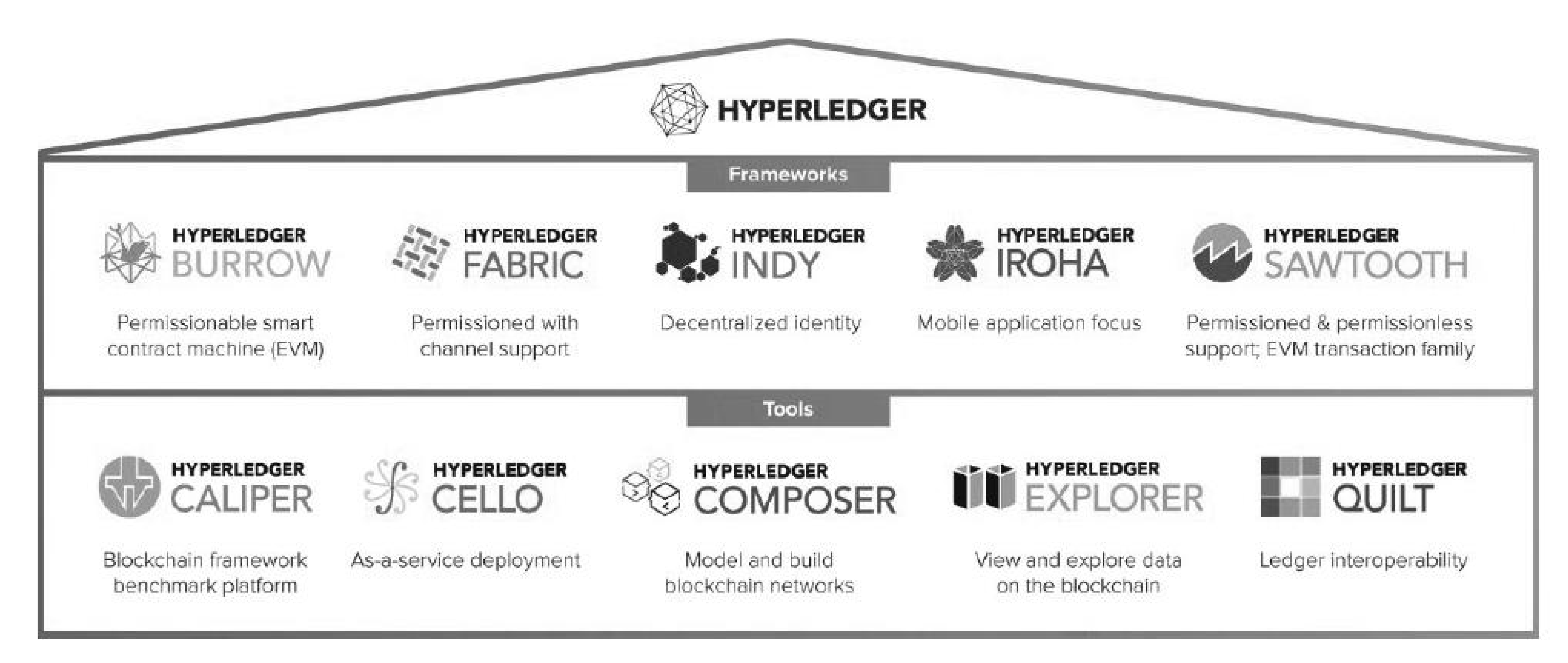


图 4.4　Hyperledger 大家庭

更详细的介绍,这里不再赘述。

Indy 是一个着眼于解决去中心化身份认证问题的技术平台,该项目由 Sovrin 基金会牵头。Indy 可以为区块链系统或者其他分布式账本系统提供基础组件,用于构建数字身份系统,它可以实现跨多系统间的身份认证、交互等操作。

Iroha 可以简单方便地以模块的形式应用于任何分布式账本系统中,其设计理念之一便是项目中的很多组件可以为其他项目所引用,同时 Iroha 区别于其他 Hyperledger 项目的一大特点是主要面向于移动应用。

Sawtooth 是一个支持许可(permissioned)和非许可(permissionless)部署的区块链系统,是功能完整的区块链底层框架。它提出的共识算法——时间流逝证明(PoET,Proof of Elapsed Time),开创性地使用了可信执行环境(TEE,Trust Execution Environment)来辅助共识达成。PoET 可以在容忍拜占庭攻击的前提下,降低系统计算开销,是较为高效且低功耗的共识算法。Sawtooth 可以应用于多种场景,包括金融、物联网、供应链等。

Caliper 是一个区块链性能基准测试工具(benchmark tool),开发者可以使用该工具内置的测试用例来测试区块链每秒执行交易数(Transactions Per Second,TPS)、延迟(latency)等性能。

Cello 是一个区块链的模块工具包,主要用于管理区块链的生命周期,在各种物理机、虚拟机、Docker 等基础设施上提供有效的多租户链服务。可用于监控日志、状况分析等。

Composer 是一个开发工具框架,协助企业将现有业务和区块链系统集成。开发人员可以借助 Composer 快速创建智能合约及区块链应用。通过强大的区块链解决方案,推动区块链业务需求的一致性。

Explorer 是一个区块浏览器,提供一个简洁的可视化 web 界面。用户可通过该工具,快速的查询每个区块的内容。包括区块头中区块号、哈希值等信息,也包含每笔交易的读写集等具体内容。

Quilt 通过实施跨账本协议(Interledger Protocol,ILP)提供分类账系统之间的互操作。ILP

主要是支付协议，旨在跨分布式分类账和非分布式分类账中传输价值。

以上所有项目都遵守 Apache V2 许可，并约定共同遵守如下基本原则：

- 重视模块化设计：包括交易、合同、一致性、身份、存储等技术场景；
- 重视代码可读性：保障新功能和模块都可以很容易添加和扩展；
- 可持续的演化路线：随着需求的深入和更多的应用场景，不断增加和演化新的项目。

Hyperledger Fabric（本书后续在没有歧义的情况下简称 Fabric）是超级账本项目中的基础核心平台项目，它致力于提供一个能够适用于各种应用场景的、内置共识协议可插拔的、可部分中心化（即进行权限管理）的分布式账本平台，是首个面向联盟链场景的开源项目。本节以 Hyperledger Fabric 为例讲述该项目的核心思想、整体架构、关键技术。

1. 核心思想

Fabric 是一个带有节点许可管理的联盟链系统。在传统的区块链系统中，系统对节点的加入没有限制，这使得系统的治理非常复杂。为了利用区块链的特性，同时避免复杂的系统治理，Fabric 采用了带有许可认证的节点管理方式，也就是系统是在一系列已知的、具有特定身份标识的成员之间进行交互。虽然对于系统来说节点本身身份是已知的，但是节点之间并不互相信任，所以节点之间还是需要一个一致性的算法来保证数据是可信的。区别于比特币等公链系统的 PoW 算法，在节点可知的 Fabric 系统中，可以采用传统的类似于 BFT 的共识算法。

Fabric 另外一个具有创新意义的做法是采用“执行-排序-验证-提交”模型。传统的区块链系统采用的是一种顺序执行的方式，交易是在排序完成之后或者是排序的过程中执行智能合约（order-excute-update）生成的，这使得所有节点都必须要按顺序执行智能合约，限制系统的可扩展性和性能。Fabric 使用了一种不一样的架构，被称为“执行-排序-验证-提交”，使得 Fabric 有更好的扩展性和灵活性；而且交易预先执行的方式避免了非确定性的状态，也使得系统能够抵抗一些恶意攻击，如资源耗尽。在这样的模型基础上，Fabric 能够将交易拆分为构建区块和更新状态两个阶段，一方面使得系统可以将交易的执行、排序、提交单独剥离出来，让系统的架构更加灵活；另一方面也使得系统架构更加具有扩展性，开发者可以针对不一样的企业需求，对执行、排序、验证、提交各个阶段定制不一样的服务。

2. 整体架构

在前面的设计思想基础上，Fabric 充分利用了模块化的设计、容器技术和密码学技术，使得系统具有可扩展、灵活和安全等特性。总的来说，在具体架构设计上它主要采用了以下的几个核心思想：

（1）灵活的链码（Chaincode）信任机制。在 Fabric 系统中，链码即智能合约。链码的运行与交易背书、区块链打包在功能上被分割为不同节点角色完成，且区块的打包可以由一组节点共同承担，从而实现对部分节点失败或者错误行为的容忍。而对于每一个链码，背书节点可以是不同的节点，这保证了交易执行的隐私性、可靠性。

（2）高效的可扩展性。相比于其他区块链系统中所有节点对等的设计方式，Fabric 中交

易的背书节点与区块链打包的 orderer 节点解耦,这能保证系统有更好的伸缩性。特别是当不同链码指定了相互独立的背书节点时,不同链码的执行将相互独立开来,即允许不同链码的背书并行执行。

(3) 隐私保护。为了保护用户、交易的隐私及安全,Fabric 制订了一套完整的数据加密传输、处理机制。同时,通过将不同的业务或用户通过通道(Channel)隔离,实现数据的隔离,从而进一步保护隐私。

(4) 共识算法模块化。系统的共识由 orderer 节点完成,并且在 Fabric 允许各类共识算法以插件的形式应用于 orderer 节点,比如 Solo 共识、Kafka 共识、PBFT 共识等。

从系统逻辑架构的角度来看,Fabric 系统主要提供成员管理、区块链服务、智能合约服务、监听服务等功能。Fabric 的系统逻辑架构见图 4.5,各个服务的介绍如下。

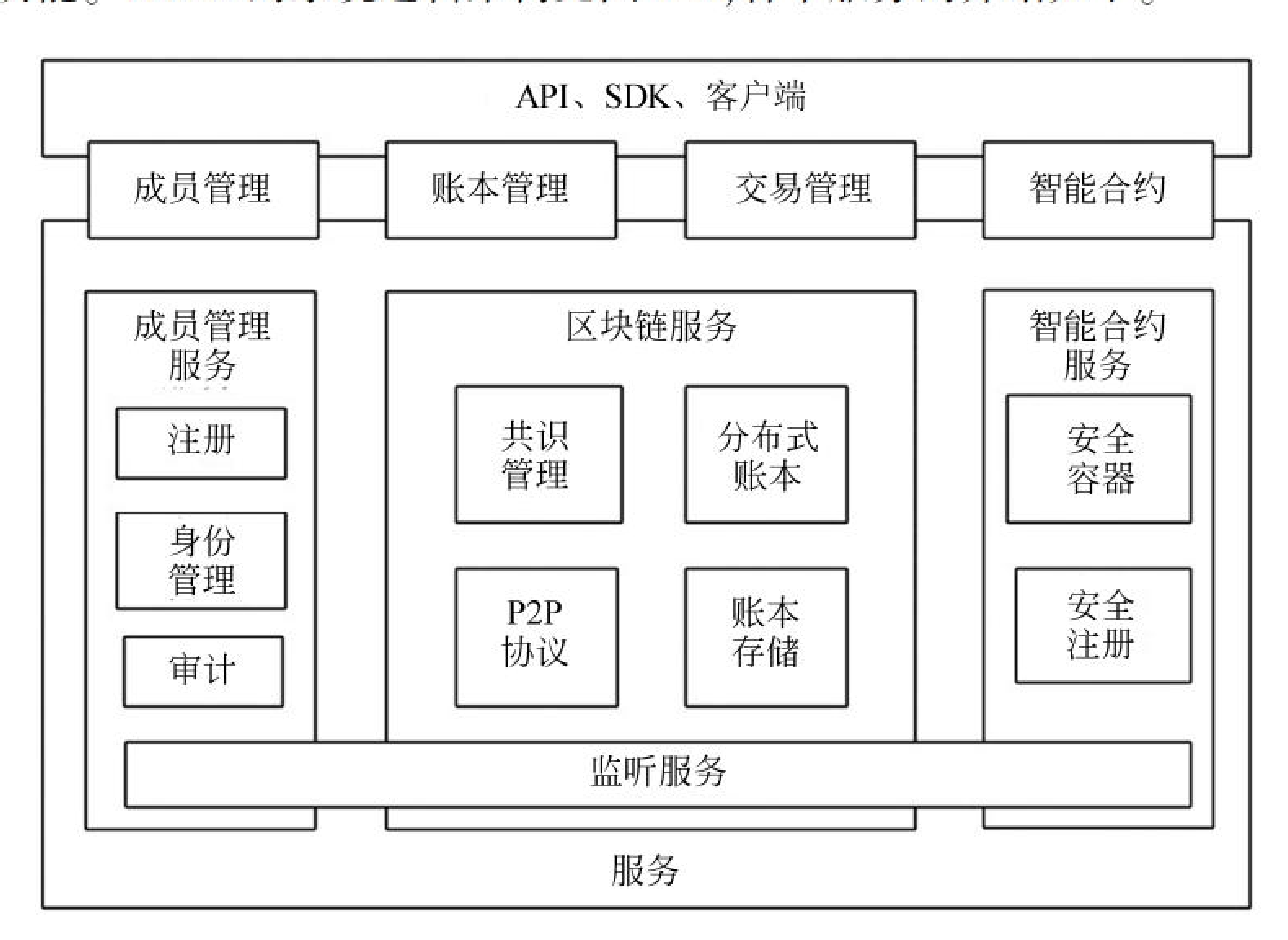


图 4.5　Fabric 系统逻辑架构

(1) 身份管理

身份管理为网络节点提供了管理身份、隐私、机密和审计的功能。Fabric 采用了 PKI 公钥体系,每一个网络节点首先需要从证书颁发机构(CA)获取身份证书,然后使用身份证书加入 Fabric 网络。节点发起操作的时候,需要带上节点的签名,系统会检查交易签名是否合法以及是否具有指定的交易或者管理权限。

(2) 账本管理和交易管理

区块链服务主要包含交易管理和账本管理。Fabric 中客户端提交交易请求,背书节点进行背书,通过共识管理模块将交易排序打包生成区块文件,主记账节点获取到区块之后,通过 P2P 协议广播区块到不同的记账节点中,拿到区块之后,记账节点通过账本存储管理模块写入本地账本中。上层应用程序还可以通过账本管理模块来查询交易,包括通过交易号、区块

编号、区块哈希值等。

(3) 链码管理

Fabric 采用 Docker 作为其链码的安全执行环境。一方面可以确保链码执行和用户本地数据隔离,保证安全,另外一方面可以更容易支持多种语言的链代码提供智能合约开发的灵活性。

从系统部署架构的角度来看,Fabric 系统常见的网络部署架构如图 4.6 所示,在常见的部署方式中,Fabric 区块链系统一般是由多个组织构成的,每一个组织有自己的 orderer 节点、背书节点、主节点和记账节点。系统中主要包含 CA、客户端、orderer 节点和 peer 节点。其中 orderer 节点功能比较单一,主要完成交易排序的功能。Peer 节点根据不同功能可以划分为背书节点、记账节点、主节点。某一个 peer 网络节点可能有多个功能,因为 peer 节点的功能独立,这也使得节点的加入和退出比较灵活。

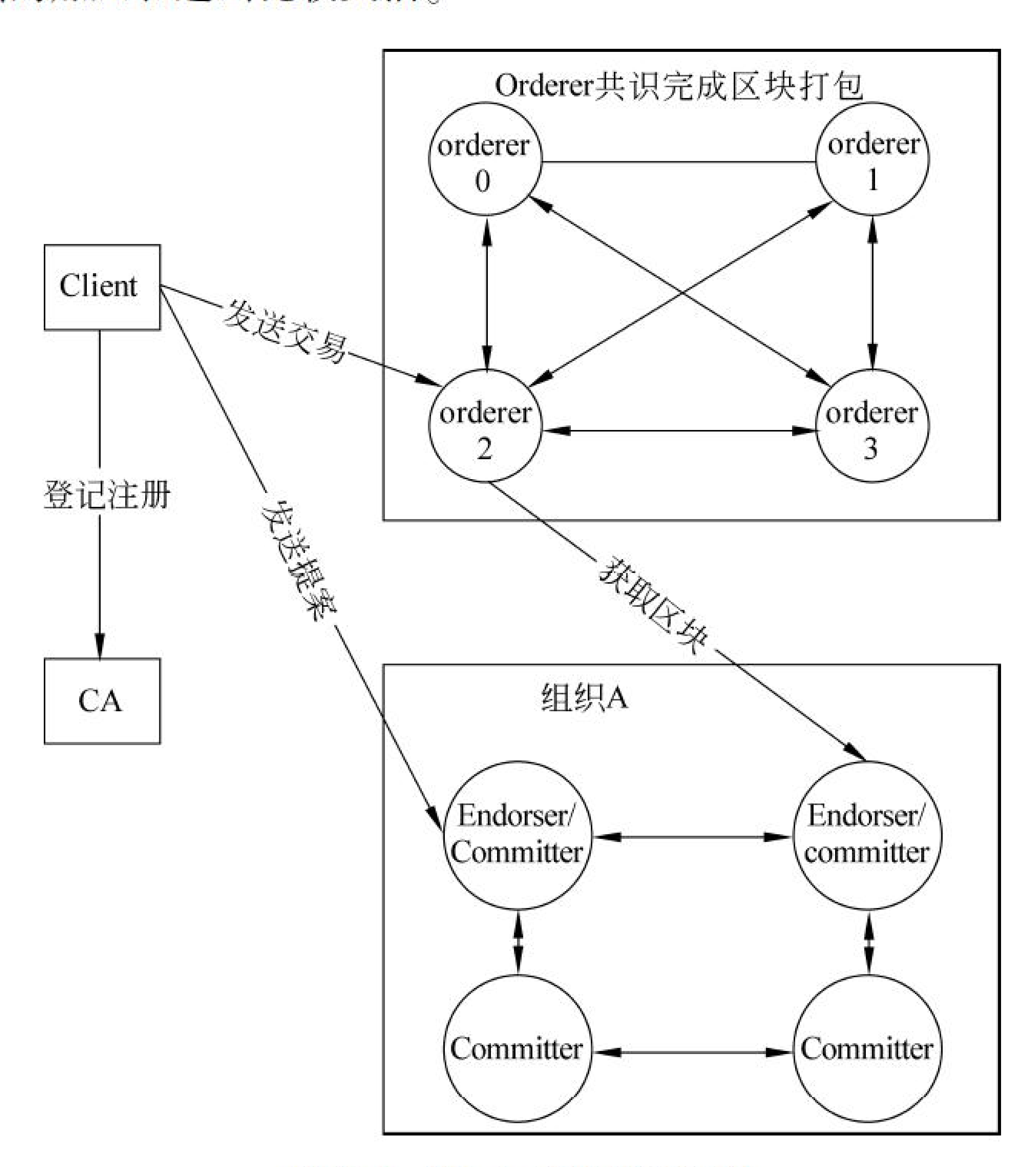


图 4.6　Fabric 系统部署架构

Peer 节点:Peer 节点是整个 Fabric 系统中的核心节点,同时承担着 endorser 和 committer 两个角色,其具体作用分别如下。

- 被某个客户端指定的 endorser 需要完成相应交易提案的背书处理。具体的背书过程为:收到来自客户端的交易提案后,首先进行合法性和权限的检查,若检查通过,则 endorser 在其本地对交易所调用的链码进行模拟运行,并对由交易导致的状态变化进

行背书并返回结果给客户端。

- Committer：负责维护区块链账本结构，对区块进行落盘。

主节点：该节点会定期从 Orderer 获取排序后的批量交易区块结构，对这些交易进行落盘前的检查，并最终对交易进行落盘（写入账本）。一般主节点也是记账节点。

Orderer：负责对交易进行排序的节点。Orderer 即为网络中所有合法交易进行全局排序，并将一批排序后的交易组成区块结构，传送至 committer 进行区块落盘的动作。

CA：负责网络中所有证书的管理，实现标准的 PKI 架构。

客户端（client）：客户端是调用 Fabric 服务的节点。要发出一个对 Fabric 系统的访问，首先客户端需要获取合法的身份证书来加入 Fabric 网络内的应用通道。客户端在发起交易时，首先要构造交易提案（Proposal），提交给 endorser 进行背书。在收集到足够的背书后，可以组装背书结果构造一个合法的交易请求，发给 orderer 进行排序处理，orderer 排序确认后再最终被发至 committer 完成交易的落盘。

3. Hyperledger Fabric 交易流程

区别于比特币的 UTXO 模型，Fabric 项目使用的模型是账户/余额模型。类似于日常所使用的银行卡，银行系统记录了银行卡对应账户所剩余的余额，当我们需要使用银行卡去交易的时候，银行会在批准交易前检查以确保我们有足够的余额。账户余额模型更加的简单和高效，基于 Fabric 的智能合约开发者可以直观地根据账户是否有足够余额来判断交易是否可以进行，因此也可以开发出更加复杂的智能合约。

在 Fabric 中账户信息存储在称为世界状态（World State）的对象中。世界状态代表了当前账本所有账户的最新值，用户可以直接根据账户获取最新的账户信息最新值，而不需要遍历整个区块文件进行计算。在实际实现中，Fabric 世界状态是通过 key-value 对象存储的，每一笔交易都会对世界状态中某个/多个 key 值进行读取、更新或者删除操作，Fabric 将这种交易结果抽象成读写集对象。读集包含了链码（智能合约）中对世界状态中 key 的所有读操作以及对应读操作读取到的版本，版本用对应 key 最后一次合法交易更新的交易所在区块编号和交易编号表示；写集包含了待更新的所有 key 和对应的 value。Fabric 利用交易的读写集来保证对世界状态更新的全局一致性。整个交易的过程如图 4.7 所示。

（1）客户端 SDK 发送提案给 endorser，提案中包含调用者的签名和应用程序生成的交易号，endorser 和 committer 可以通过交易号检查是否有重复的交易。

（2）Endorser 调用对应的链码程序执行交易操作，生成读写集。链代码程序会查询世界状态中对应的 key 值生成读集，然后执行一系列链代码中所写的业务逻辑，最后计算出对世界状态中的 key-value 更新。Endorser 对这个过程进行记录，最后的结果生成了一个读写集对象。

（3）Endorser 将背书结果返回给客户端 SDK，其中包含了读写集对象。

（4）客户端 SDK 将包含读写集的背书结果打包成交易发送给 orderer。

（5）Orderer 会接收到来自不同客户端的并行交易，它在内部将交易排序编号，然后组装

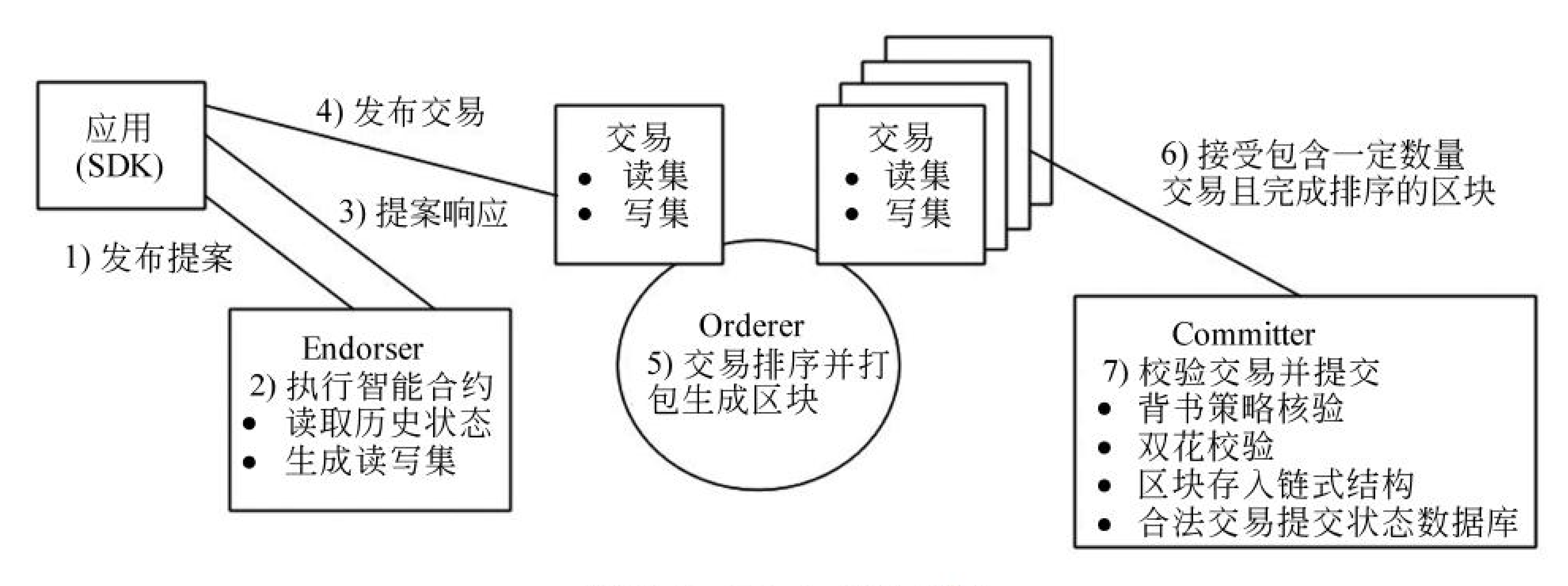


图 4.7　Fabric 交易流程

成区块。

（6）Committer 从 Orderer 拉取区块。

（7）Committer 验证区块合法性。例如验证交易是否符合背书规则,交易是否存在双花等。如果交易验证通过,则将区块写入到本地的区块链账本,同时将区块中合法的交易包含的写集内容写入到世界状态数据库中。这样一次完整的交易就完成了。

4. Hyperledger Fabric 共识设计

共识服务在 Fabric 系统中占有十分重要的地位。所有交易在发送到 Fabric 系统中以后,都要经由共识服务对交易顺序进行共识,然后将交易按序打包进入区块链,保证了任意一笔交易在区块链中的位置,以及在整个 Fabric 系统中各节点的一致性和唯一确定性。

在 Fabric 1.0 版本以前,共识服务并未分离成独立的功能模块。Fabric 1.0 版本以后,共识服务被抽象成了单独的功能模块,称之为 orderer 模块,可以独立对外提供共识服务。同时,orderer 模块定义了共识服务的标准接口,以供开发者开发新的共识方法来支撑共识服务。

当前官方 Fabric 共识服务主要支持的有 solo 和 Kafka 两种共识算法,社区曾经在 1.0.0 的 alpha 版本中尝试加大对 PBFT 共识方法的支持,该方法是简化的 PBFT 共识方法。这几种算法简要介绍如下:

- Solo:提供单节点的排序功能。只能起一个节点,只是为了测试使用,不能进行扩展,也不支持容错,不建议在生产环境下使用。
- Kafka:提供基于 Kafka 集群的排序功能。支持 CFT,支持持久化,可以进行扩展,是允许 CFT 情况下 Fabric 当前推荐在生产环境下使用的共识方法。
- PBFT:实用拜占庭容错算法是一种状态副本复制算法,不同共识节点保存了一个状态机副本,副本里面保存了服务的操作和状态。在系统可能存在 f 个失效节点的情况下,如果能保证系统总的节点个数大于 3f+1,那么在 PBFT 算法下系统总能达成一致状态。

从模块内部细分看,共识服务 orderer 模块主要包含对外接口、共识方法、共识账本、公用

模块,其架构如图 4.8 所示。

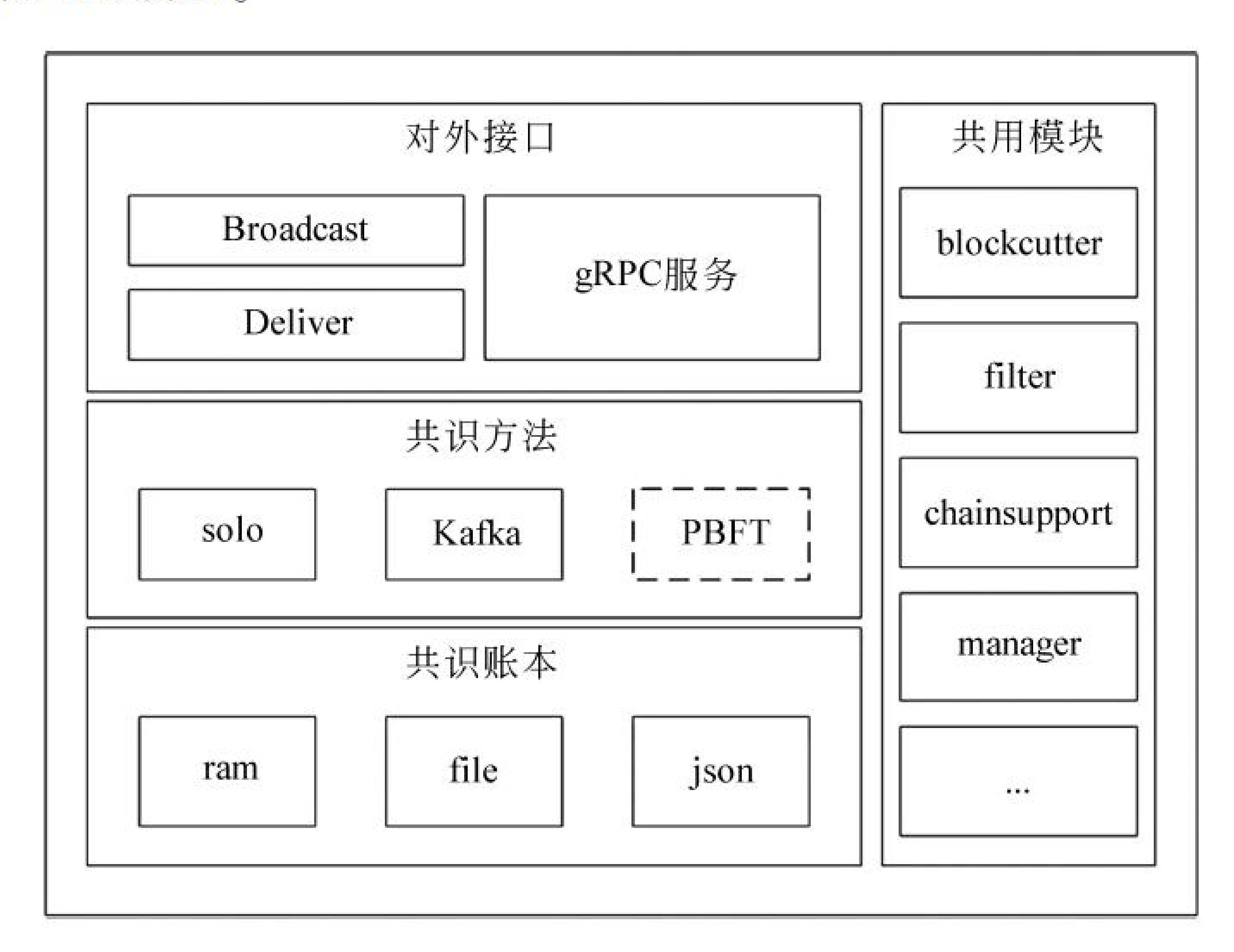


图 4.8　Fabric 共识模块架构

- 对外接口：主要包括 Broadcast 和 Deliver 两个接口,分别用于接收客户端发来的交易和处理 Fabric 系统中的各类节点发来的获取区块的请求。
- 共识方法：主要用于对接收到的交易进行排序,保证交易在区块链中的顺序在 orderer 模块的所有节点里是一致的。目前,开源 Fabric 系统中主要依靠 solo 和 Kafka 两种共识方法实现。
- 共识账本：主要用于提供区块链的存储方式,当前支持 ram、file 和 json 三种方式存储区块链,其他模块可以通过简单接口存入或者读取区块链。
- 公用模块：主要用于为其他基础模块提供一些公用功能,包括 blockcutter、filter、chainsupport、manager 等。

5. Hyperledger Fabric 智能合约

智能合约是区块链的重要组成部分之一,在 Fabric 系统中,智能合约被称之为链码。链码分为两类,分别是系统链码和用户链码。

系统链码是主要实现系统管理的功能,他主要提供系统内置的功能,因为在系统中内置,减少了链码和背书节点通信的开销。主要包括生命周期管理链码(LSCC)、配置管理链码(CSCC)、查询管理链码(QSCC)、交易背书链码(ESCC)和交易验证链码(VSCC),其功能分别介绍如下：

- LSCC:管理在背书节点上的链码部署。主要包括链码的安装、实例化、升级。
- CSCC：管理在 peer 侧的配置。包括加入新的通道和查询给定通道的对应配置。
- QSCC:提供查询记账节点的账本数据的功能,包括区块、交易数据和区块链信息。其

支持的接口包括 GetTransactionByID(根据交易号查询交易)、GetBlockByNumber(根据区块号获取区块)、GetBlockByHash(根据区块哈希获取区块)、GetBlockByTxID(根据交易号获取区块)和 GetBlockChainInfo(根据通道名称获取最新区块链信息,例如账本高度等)。

- ESCC:提供对交易结果的转换和对交易进行背书的功能。
- VCSS:主要是在记账前提供区块和交易的验证功能。

用户链码是用户编写的智能合约。Fabric 支持使用 Golang、Node. js、Java 语言来编写链码,这些语言对大多数应用开发者来说并不陌生,能够快速上手,有利于区块链应用的快速开发。链码运行在容器中,使得智能合约的执行和 endorser 进程及账本分离开来。在 Fabric 系统中,以及用户链码的整个生命周期中,用户链码主要有开发、安装、实例化、升级、运行 5 个阶段。各阶段简要介绍如下:

- 开发:用户基于 Fabric 所提供的链码接口(ChaincodeStub)操作状态数据块以完成智能合约代码。最终形成的是 Golang 或者其他语言的代码文件。
- 安装:管理员指定链码的名称和版本号,调用 SDK 将链代码文件打包发送给 endorser。Endorser 将链码包以链码名称和版本号的组合形式(例如 mychaincode. 1.0),存储在本地特定的目录下。在很多公有云服务供应商提供区块链服务的情况下,链码的安装和后续实例化及升级都可以一键完成,增强了区块链的易用性。
- 实例化:管理员指定通道、链码名称、版本号、背书策略和链码初始化函数,向 endorser 发起实例化请求,endorser 从本地链码包获取链码文件。根据不同的链码语言,endorser 使用对应语言的编译器编译链码文件,进而生成可执行文件,并将可执行文件打包生成一个 Docker 镜像,然后使用该镜像创建一个运行对应链码的容器。链码启动后和 peer 之间通过 gRPC 进行通信。
- 升级:链码升级过程主要是使用新的链码文件上传到 endorser,然后生成新的链码镜像和容器的过程。链码名称必须要保持一致,链码版本号必须是不一样的,但是没有大小规则,也就是最后升级的链码就是最新的。
- 运行:在运行阶段,链码主要完成用户的交易操作。用户通过 gRPC 向 endorser 发起对应链码的调用请求,endorser 将请求转发给链码。链码执行智能合约逻辑,在此过程中,它会有多次和状态数据进行交互的过程。包括从 endorser 状态数据库中读取特定的值和向 endorser 状态数据库中写入特定的值。

目前 Fabric 没有提供对链码的停止和启动操作。当链码本身写的有问题时,链码可能会发生异常,最终导致链码容器退出。用户需要自己通过 Docker 来管理链码生命的终止。

6. Hyperledger Fabric 安全及隐私保护

区块链的安全和隐私主要体现在下面几方面的需求:交易数据安全保密、不可更改,交易匿名,符合监管和审计的要求。为了满足这些需求,Fabric 采用了密码学相关的技术,包括对称加解密、非对称加解密、数字摘要等。

如图 4.9 所示,为了实现更加灵活的安全隐私服务,Fabric 将安全服务模块化划分为通道管理、通信管理、身份管理、区块链密码服务管理模块。

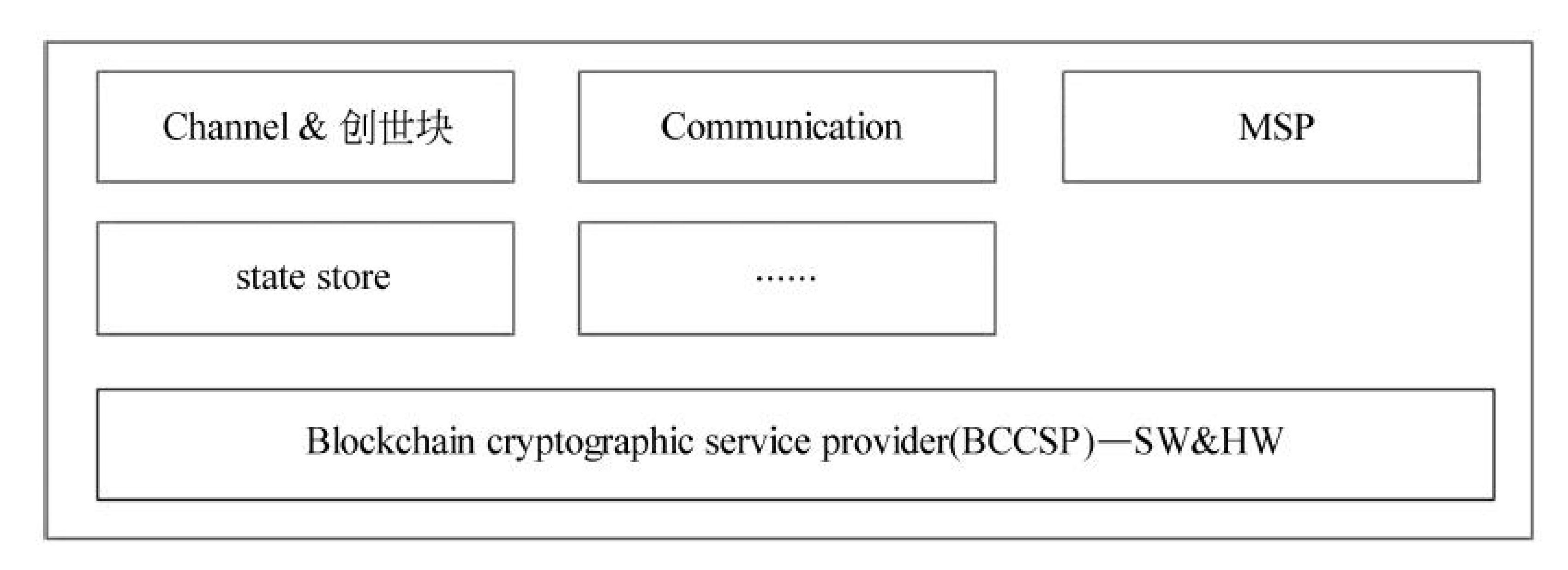


图 4.9 Fabric 安全服务模块

- BCCSP 服务:区块链密码服务管理,它提供了一组密码学的工具,通过这个工具集来实现上面应用层的数据安全和隐私保护。它提供了包括非对称加密(RSA)、块加密算法(AES)、椭圆曲线签名(ECDSA)、哈希算法(HASH)、哈希消息认证码(HMAC)、X509 证书、标准的安全接口(PKCS11)等算法。比如,为了支持国密算法,则需要扩展 BCCSP 服务。
- 通道管理服务:通道(channel)是 HyperLedger Fabric 的一种保护机制,用于交易参与方安全地和 Peer 进行通信而对其他参与方不可见,另外对于一个通道而言具备自己独立的服务空间,也就是说背书、链码、链码执行环境都是独立的,部署和升级链码也只是影响当前的通道。管理员通过通道配置文件(configtx.yaml)创建创世块,创世块里面保存了一些配置和安全标识;创世块会被客户端从 endorser 获取回来,作为加入通道的依据。
- 身份管理服务:身份管理服务(Membership Service Provider,MSP),通常直译为成员关系服务提供者。作用类似于,在一个运行的 Fabric 系统网络中有众多的参与者,MSP 就是为了管理这些参与者,辨识验证哪些人有资格,哪些人没资格,既维护某一个参与者的权限,也维护参与者之间的关系。MSP 中也使用了 BCCSP 提供的密码学服务,因为 MSP 维护了参与这个的权限,一旦泄露,对系统可能产生不可估量的损失。
- 通信管理服务:不同节点之间通信是通过 gRPC 通信的,主要通过安全传输层(Transport Layer Security,TLS)来保证信道的安全。

7. Hyperledger Fabric 应用开发

关于 Fabric 应用的设计开发,图 4.10 是 Fabric 的参考应用架构。通常区块链应用可分为呈现层、应用层、业务层和数据层。

- 呈现层:呈现层包含了我们通常所说的用户界面,比如注册界面、交易界面、应用管理界面等,这一层和传统的 Web 应用和移动 App 并无差别,用户在这一层中对区块链的存在无感知。

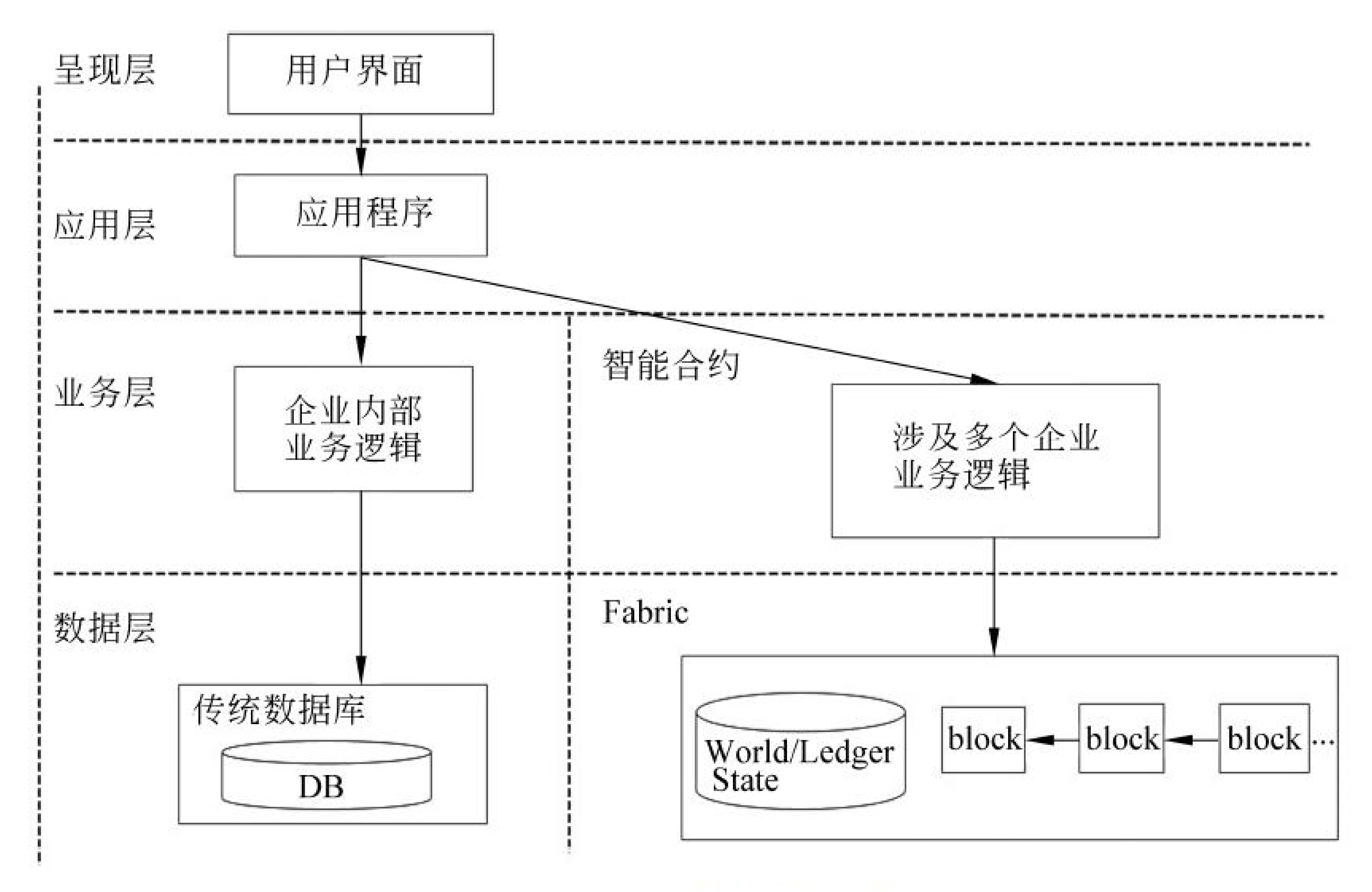


图 4.10　Fabric 的参考应用架构

- 应用层：应用层为应用逻辑所在的一层。这一层处理用户输入数据，根据这些数据判断出具体的业务，然后调用相应的业务处理接口。如果为企业传统内部业务则通过传统的业务接口（如数据库）处理，如果为区块链业务则通过区块链智能合约调用接口处理。
- 业务层：业务层封装了 Fabric 应用的全部业务逻辑，是整个应用的核心部分。业务层可分为两类：企业内部传统业务逻辑和跨企业/区块链业务逻辑。企业传统内部业务逻辑和传统应用业务逻辑实现方法一样，跨企业/区块链业务逻辑则由智能合约具体实现。
- 数据层：数据最终的存储是在数据层。数据层分为传统数据库存储和 Fabric 存储。企业内部逻辑的数据会存在传统数据库中，这部分数据是企业内部隐私数据。另外涉及多个企业业务逻辑的数据则存在 Fabric 区块链中，各企业间通过 Fabric 区块链共享这些数据。

总的来说，相对于其他区块链平台，Fabric 具有如下的几点拓展性和优化性。

- 高效的可拓展性：相比于其他区块链系统中所有节点对等的设计方式，Fabric 中交易的 endorser 与区块链打包的 orderer 节点解耦，这将保证系统有更好的伸缩性。特别是当不同链码指定了相互独立的 endorser 时，不同链码的执行将相互独立开来，即允许不同链码的背书并行执行。
- 更强的隐私保护：为了保护用户、交易的隐私及安全，Fabric 实现了一套完整的数据加密传输、处理机制。同时，其特有的智能合约执行流程也对用户隐私进行了一定程度的保护。

- 可插拔的共识算法：Fabric 系统将共识交由 orderer 节点完成，并且允许各类共识算法以插件的形式应用于 orderer 节点，从而使用户能够根据具体的应用场景选择不同类型和特性的共识算法。

4.5 本章小结

区块链自诞生于比特币以来，就以一个独立于比特币的脉络向前发展。本章第一节以时间为索引，概括性地描绘了区块链技术的发展历程。第二节以区块链平台的迭代为索引，阐述了区块链到目前为止的三代平台类型。第三节则以参与者的不同关系为索引，说明了区块链的三种组成形态，分别是公有链、联盟链和私有链。最后，本章以比特币、以太坊和超级账本为代表，介绍了三种不同框架的关键技术和特性。本章以宏观的视角，帮助读者俯瞰区块链技术，对区块链进行系统的了解。

第5章
区块链技术趋势

区块链里有一个三元悖论，三元是说衡量区块链好坏的三个指标：高效性、去中心化和安全性。悖论是讲这三条不可能同时取得最佳，提高其中某一个的指标必然以损害另外一个或者两个作为代价。

这三条又要区分对待。安全性最重要，区块链的不可篡改性决定了对错误的零容忍，将错就错只能是不得已的选项，最好没有任何错误。安全性不能退让，只有越变越好一条路。安全级别高，剩下的办法是在高效性和去中心化之间寻求平衡。去中心化虽然是区块链最重要的一个特性，但在实践中可以适当弱化，以“准去中心化”或者是“多中心化”来换取高效。

除了三元悖论，多链并存的现状也是困扰区块链的一大问题。没有哪一个或者哪几个区块链系统优秀到足以覆盖其他所有系统，所以，跨链仍然是一个不可回避的问题。

区块链的从业者试图从技术上解决这些难题，本章将分别从性能、安全隐私、跨链以及图结构这些方面来讨论区块链技术。

5.1 区块链性能

5.1.1 当前存在的问题

比特币诞生时还只是黑客的玩具，对其有了解的人还很少。随着比特币知名度的提高，越来越多的交易涌向比特币系统，其性能问题就凸显了出来：交易确认时间久，吞吐量低。比

特币每 10 分钟出一个区块,区块最大为 1MB,换算下来就是每秒钟可以处理的交易数是 7 笔,这与当前很多的金融系统相比实在太少。

吞吐量过低是比特币系统的严重问题,这会大大限制其可用场景。后来为数不少的公链项目都以改进性能为首要目标,或者增加区块大小,或者提高出块频率。在比特币的框架下,靠调整这类参数虽然可以一定程度上改善吞吐量,但其上限也就是每秒几百笔交易,很难有本质上的突破。而作为联盟链代表的 Hyperledger Fabric,其吞吐量也只有每秒几百到几千笔交易的量级,并不能满足当前金融系统对吞吐量(几万笔交易每秒)的需求。

吞吐量过低的根因,其实在于共识过程。在一个完全去中心化的环境里,要得到多数节点认可,往往需要多次交互,而每次交互又均伴随着网络延迟,在此两者的共同影响下,区块链系统的吞吐量注定难以提高。

但是,总有另辟蹊径的人。

5.1.2 常用解决方法

1. 异步共识

在共识协议里,主流的做法是每出一个块,所有节点之间要进行同步,共识通过以后再继续出下一个块。另有一类做法是出块以后无须立即达成共识,每个节点在遵循某种规则的前提下,尽最大的能力出块。如果规则制定得足够巧妙,各自为战的节点在经过一段时间之后,仍然可以达成一致。

这就是著名的异步 Graph 算法。IOTA、HashGraph 就是其中的佼佼者。Graph 算法比较复杂,后续另辟一节详细介绍(见第 5.4 节)。

2. 随机共识

全网所有节点参与共识效率较低,那么一个提高性能的直接想法就是用部分节点间的共识代替全网共识。然而,如何证明“部分” =“全部”呢? 其实,这个证明并不存在。但是,“部分”能否极大程度地代表“全部”呢? 这个其实有解决办法:如果“部分”是完全随机地从节点中抽取,在达到一定样本量时,统计学上是可以表达“全部”意义的。

Algorand 算法在“随机抽取”上研究了一套算法,将整个共识过程分为若干步骤,每个步骤随机选举出若干节点组成的委员会,由这个委员会完成共识。而下一个步骤又是随机选出的另外一个委员会,在更长的时间跨度内,实现了公平,也达到了高效共识的目的。

可验证随机函数(Verifiable Random Functions, VRFs)是 Algorand 算法的核心,每个节点凭此函数获知是否在加密抽签中获胜。获胜的用户进入“验证者”委员会,接下来的共识过程便可以在“验证者”中直接完成。

Algorand 有近乎完美的数学设计。但因流程较为复杂,使其在实际网络中的表现还有待验证。

3. 分区方案

区块链系统,单纯从数据存储的角度来看属于分布式日志数据库。那么,分布式日志数

据库中用来提高性能的方案理应可以用于区块链系统。数据库的技术已经非常成熟,在处理大数据时,分区是不二选择。所以,区块链系统理应也可以分区。

怎么分区是分区方案的关键,可以选择的方式有很多：按交易发送者地址分,按交易 ID 分,按交易类型分,按地域分,按市场分等。分区技术的瓶颈是跨区数据交换,数据交换主要受限于网络带宽。另外,特别地针对区块链系统,交易之间冲突的解决、不可篡改特性的保证以及交易确认时间不能过长都将是区块链分区方案所面临的直接问题。不过,分区依然是很有前途的方案,但这方面的研究,甚至是产品并不多,原因是实现难度大,同时对智能合约的使用限制明显。

需要指出的是,以太坊的分片并不是分区技术。分片更接近下面说的子链,每一个片是内部耦合度很高的自治区,片与片之间的数据交换较少;而分区同属于一个整体,区与区之间的数据交换量较大。

4. 子链/侧链技术

一条链的区块链系统性能较差,那么一个直观的想法就是多链并行可以提高区块链系统的性能表现。闪电网络(Lighting Network)是子链技术的代表：它指的是 A 和 B 两人用多重签名的方式冻结自己的比特币,然后进行链下交易,交易参与方可以随时关闭交易通道,关闭时的余额信息会写回比特币区块链。

闪电网络是基于比特币的扩展。还有走得更远的方案,类似于银行结算系统,交易在某个子链内发生,只有最后结算的信息回写到主链。这个子链可以是某个很大的市场,比如淘宝、京东等,而主链则可以对应银联。

5. 可信执行环境

如果某类节点的运行环境具备如下特征：要么不运行,一旦运行必然可靠,无法被外界做任何修改,那么这类环境便可称为可信执行环境。基于可信执行环境假设而设计的共识可以进行一定程度上的简化,因为不必考虑节点,可以任意篡改共识逻辑,也就是不必考虑拜占庭攻击,所以通常应用可信执行环境可以提高区块链的性能表现。

6. 隐形中心化

区块链界有一种说法：完全去中心化并无必要,受限制的中心化更贴合现实情况。具体来说,受限制的中心化可以是多个中心,也可以是中心节点轮换的形式。

典型地,DPoS 就是中心轮换的共识算法。EOS 便采用了 DPoS 共识算法,其中的超级节点权力很大,已经有了中心化的特征,可以看作是区块链系统对于去中心化这一特性的妥协。

而实际上,大多数共识协议都或多或少会引入一些隐形中心化的假设。如果协议中有“领导者”“超级”“委员会”这类概念,那么其实就已经赋予了某些节点以特权。在现在的区块链技术发展阶段,如果能改善性能,受限制的特权(前提是特权没有大到拥有绝对的控制力)还是可接受的。

5.2 区块链隐私保护

5.2.1 当前存在的问题

区块链是一个分布式账本，具有公开、透明、不可篡改等优点。但区块链应用到现实商业世界的时候，还有很多问题亟待解决，首当其冲就是隐私保护问题，如何解决公开、透明与隐私保护之间的矛盾，一直是区块链技术发展的重要方向，至今仍未完全解决。

比特币有较好的匿名性，是因为比特币的账户地址，是以非对称密钥的公钥经过一系列运算得到的。比特币在网上传输的所有交易，都是公开的，也就是没有隐私。普通民众，很难把公钥和真实世界的人的身份对应起来，从而给人造成一种比特币隐私保护能力较好的“假象”。

例如银行间转账，采用区块链系统来记录交易过程，虽然严格一致的账本，省去了繁杂的对账工作，但没有任何一家银行希望自己的资金往来，完全暴露在众目睽睽之下。在使用区块链联盟链的场景下，虽然交易不会被公众知晓，仅仅是联盟内成员可见，但依然是不可接受的。试想联盟内存在 A、B、C 三家银行，A 和 B 银行的资金往来，A 和 B 银行的客户账户信息，肯定不希望被 C 银行知晓。

除了在企业领域，在个人消费者领域，隐私保护的要求也越来越高。在 2018 年 5 月 25 日，史上最严格的欧盟隐私保护法案 GDPR（*General Data Protection Regulation*，《通用数据保护条例》）付诸实施。一旦有用户个人数据上链，区块链服务提供者（如果有区块链服务提供者而非公链的话），必须保证用户数据的隐私性。在 GDPR 中，规定了公民对个人信息的若干隐私保护权利，包括：知情权、访问权、更正权、被遗忘权、限制处理权、拒绝权、数据可携带权、免受自动决策权等。对于没有服务提供方，参与者完全对等的公链，例如比特币或以太坊，已经暴露一些隐私保护方面的难题：如果有人将其他人的隐私信息，以一条交易信息的附加信息的方式，记录到以太坊的公链上，则没有人可以将这条信息删除，这条信息永久存在于以太坊的公链上。

对链上数据加密，仅交易参与的双方可以解密，这可以解决大部分隐私保护的问题，但区块链系统必须直接面对这样一个问题：如何在链上数据加密的情况下，达成多方校验和共识，从而完成一笔交易。

5.2.2 常用解决方法

1. 同态加密技术

密码学中的同态加密技术被引入到区块链领域，用以保障区块链在金融交易场景的隐私性。同态加密（Homomorphic Encryption）是一种特殊的加密方法，对密文直接进行处理，与对明文进行处理后再对处理结果加密，得到的结果相同。从抽象代数的角度讲，保持了同态性。

一般包括四种类型：加法同态、乘法同态、减法同态和除法同态。以加法同态为例，它的基本思想是：如果有一个加密函数 f，满足 $f(A)+f(B)=f(A+B)$，我们将这种加密函数叫作加法同态。

在做金融转账交易时，在区块链智能合约中看到的是同态加密后的密文数据，由密文数据直接运算，得到转账后的金额。整个运算过程中的数据，包括区块链账本记录的数据，都是由同态公钥加密后的数据，只有持有对应私钥的客户端节点，才能够解密个人相关的数据，查看到明文信息，其他节点无法获取明文内容，从而保证了整个金融交易的隐私性。

目前可以达到商用水平的同态加密技术，只有加法同态技术。在世界上一些顶尖科技公司，也在发展全同态加密方案，即一个加密函数，同时满足加法同态和乘法同态。但因为乘法同态加密的性能还较差，目前还没有公开可见的支持全同态加密的商用产品。

2. 零知识证明技术

零知识证明(Zero Knowledge Proof)，是由 S. Goldwasser、S. Micali 及 C. Rackoff 在 20 世纪 80 年代初提出的。它指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。零知识证明是代数数论、抽象代数等数学理论的综合应用，如果不是数学科班出身，很难真正理解零知识证明的内部原理。在此，笔者尝试剖析其内部数学原理，感兴趣的读者可以翻阅零知识证明的基础性论文 *The knowledge complexity of interactive proof systems*①。

在区块链领域中，交易的隐私保护和交易的多方校验、共识之间的矛盾，正是零知识证明技术要解决的问题。

举一个实际的场景：利用区块链系统，多家银行组成联盟链。联盟中某银行的 A 账户给另外一家银行的 B 账户转账 100 元，我们不希望区块链系统各节点看到 A 给 B 的具体转账金额，同时，又需要确定 A 给 B 的转账是有效的。何为有效呢？①A 的当前余额足以支撑这笔转账，即 $Ac > At$(Ac：A 当前余额，At：A 转账金额)；②A 转账后剩余的金额加上转账金额，等于原来的金额，即 $Ac2 + At = Ac$(Ac2：A 转账后余额，At：A 转账金额，Ac：A 转账前余额)；③A 减少的金额，等于 B 增加的金额，即 $At = Bt$(At：A 转出的金额，Bt：B 接收到的金额)。为了保证交易金额的隐私性，A 账户给 B 账户的转账金额，在整个区块链系统中都是采用上一节提到的同态加密技术进行加密的，对于执行智能合约的节点，当它执行 A 给 B 的转账逻辑时，面对的是一堆加密过后的金额，那么如何判断以上三个条件是成立的？

在以上的场景中，可以利用零知识证明相关的技术来完成加密后交易有效性验证，结合同态加密隐私保护能力，完成完整的交易隐私保护和校验流程。

目前在区块链领域，应用的零知识证明技术有几种，包括 zk-SNARKs、ZKBoo、zk-STARKs 等，其中以 zk-SNARKs 应用最为广泛。

---

① SHAFI GOLDWASSER, SILVIO MICALI and CHARLES RACKOFF, The knowledge complexity of interactive proof systems. In Society for Industrial and Applied Mathematics, 1989, pp. 186-208.

zk-SNARKs 是在一种非常适合于区块链的零知识证明技术,它的全称是 zero-knowledge Succinct Non-Interactive Arguments of Knowledge(零知识,简洁,非交互的知识论证)。它可以实现验证节点在不知道具体交易内容的情况下,验证交易的有效性。听起来是非常不可能的事情,但确实是可实现的。感兴趣的读者,可以参阅 Zcash 的论文和博客:“Zerocash: Decentralized anonymous payments from bitcoin.”①、https://z. cash/technology/zksnarks. html②。

Zcash 是 zk-SNARKs 技术的第一个成功的商业应用,它成功实现加密数字货币交易过程中交易金额和交易方身份的完全隐藏。通过 Zcash 应用我们可以看出,zk-SNARKs 零知识证明技术具有证明材料生成慢(几十秒)、验证快(毫秒级)、证明材料体积小(288 字节)的特点。与比特币区块链系统相比,单笔交易的时延较大,但最耗时的证明材料生成过程,是在交易发起方节点完成,而链上交易的验证过程是快速的,因此系统整体吞吐率与非零知识证明加密数字货币相比并没有显著差异。

zk-SNARKs 零知识证明技术目前也在飞速发展中。在 Zcash 2017 年 9 月对 zk-SNARKs 技术的更新中,已经大幅度地提升零知识证明的计算性能,证明的生成时间由 37 秒缩短到 7 秒,证明材料生成过程中的内存消耗,也由大于 3GB 降低到 40MB。相信在不久的将来,zk-SNARKs 技术在移动设备的应用,将变得更加可行。

zk-SNARKs 技术有一个让人诟病的地方——它的算法依赖于初始的公共参数作为信任设置(trusted setup)。这个公共参数是随机数,由它来生成 zk-SNARKs 的证明公钥(proving key)和验证公钥(verify key),这个原始随机数使用完之后需要立刻销毁,一旦泄露,拥有原始随机数的人可以随意伪造证明,从而使得零知识证明的正确性荡然无存。目前,学术界采用多方安全计算的方案,来降低原始随机数泄露的概率。利用安全多方计算构造原始随机数的过程可简单描述为:每一方都生成原始随机数的一部分,多方拼凑成随机数整体,而且每一方无法知晓其他方的随机数部分,在原始随机数利用完之后,只要有任意一方销毁了自己持有的随机数部分,将无法再还原这个随机数,从而保证了整个零知识证明系统的安全。

诞生于以色列理工学院的 zk-STARKs 技术是最近兴起的区块链零知识证明技术。公开资料显示,该技术与 zk-SNARKs 技术相比,优点是不需要信任设置(trusted setup),并具有后量子安全性(在量子计算这种算力更加强劲的破解手段出现后,所应用的加密手段依然具备安全性),缺点是零知识证明材料的长度由 zk-SNARKs 的 288 字节上升至几百 KB。另外,截至目前,还未有公开项目使用 zk-STARKs 技术。

① Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, 2014, pp. 459-474.

② 查阅地址 https://z. cash/technology/zksnarks. html

3. 其他隐私保护技术

除此之外,密码学中的群签名、环签名等技术也被引入到区块链系统中,用以提升系统的隐私保护能力。群签名是验证者利用群公钥来验证签名信息的正确性,但是不能确定群中哪个成员进行了签名。虽然一定程度上保护了隐私性,但群签名中存在管理员的角色,群管理员可以最终揭示签名者。而环签名则在群签名的基础上,去掉了群管理员的角色。在区块链交易中,环签名通过模糊身份认证,只能证明签名者属于某一个组,却不知道是属于具体哪个人,从而使得区块链交易具有高度的匿名性。

可信执行环境(Trusted Execution Environment,TEE)也被用到区块链的隐私保护领域中。TEE 在系统中(包括手机终端、服务器),是一个独立的环境,受硬件机制保护,与现有系统隔离,提供从文件到内存的全方位的安全能力。它可以为区块链中密钥保护提供硬件级别的加密能力。同时,TEE 作为一个安全、可靠、中立的环境,可以用来执行区块链系统中,隐私性要求比较高的业务逻辑,比如前文提到的密文状态的交易有效性验证,在 TEE 内部,可以将密文解密成明文再进行运算,而不用担心明文数据被窃取,在数据离开 TEE 环境时,先转换成密文,再返回通用操作系统。

这里需要提一点,区块链系统仍会继承现有的中心化系统的隐私保护问题,因此,常规系统的隐私保护安全防护,在区块链系统里同样重要。同时,区块链系统应该给用户足够的安全及隐私保护提示,很多时候不是系统不够安全,而是用户把钥匙交给了黑客。因此,如何防范通过社交工程学相关的手段来破坏区块链系统的安全性及隐私性,同样是区块链设计者需要考虑的问题。

再回到本章开始提到的问题,对链上数据加密,并通过数学手段验证交易的有效性,确实能够解决区块链大部分的隐私保护难题,尤其是企业数据上链的情况。但对于个人数据的隐私保护,尤其对于 GDPR 中提到的公民对个人数据的更正权、被遗忘权,与区块链的不可篡改性依然是相冲突的。也有可能个人隐私数据上链是个伪命题——个人的隐私数据,并不适合在区块链上传播。但也有可能在不远的将来,真的出现“可篡改”的区块链,当然,区块链的篡改过程,也是在多方见证和共识下完成的。

5.3　跨链技术

5.3.1　当前存在的问题

区块链为我们带来了防篡改、去中心化、不可逆、智能合约等极具价值的特性,我们可以使用一个独立的区块链系统构建一个完美的分布式账本。但是,多条区块链之间互联互通,也是非常必要的。

在区块链最传统的加密数字货币领域,有些用户则倾向于使用比特币,有些用户则倾向于使用以太币,或者其他加密数字货币。大多数区块链加密数字货币都是独立的价值网络,

大多都无法参与自身之外的信息交互和价值转移,从某种程度上讲,可以视其为一个“信息孤岛”,区块链上的价值流通也大大的受限。这里以一个例子来描述跨链技术在加密数字货币领域的意义,见图 5.1 比特币网络与以太币网络跨链实例:

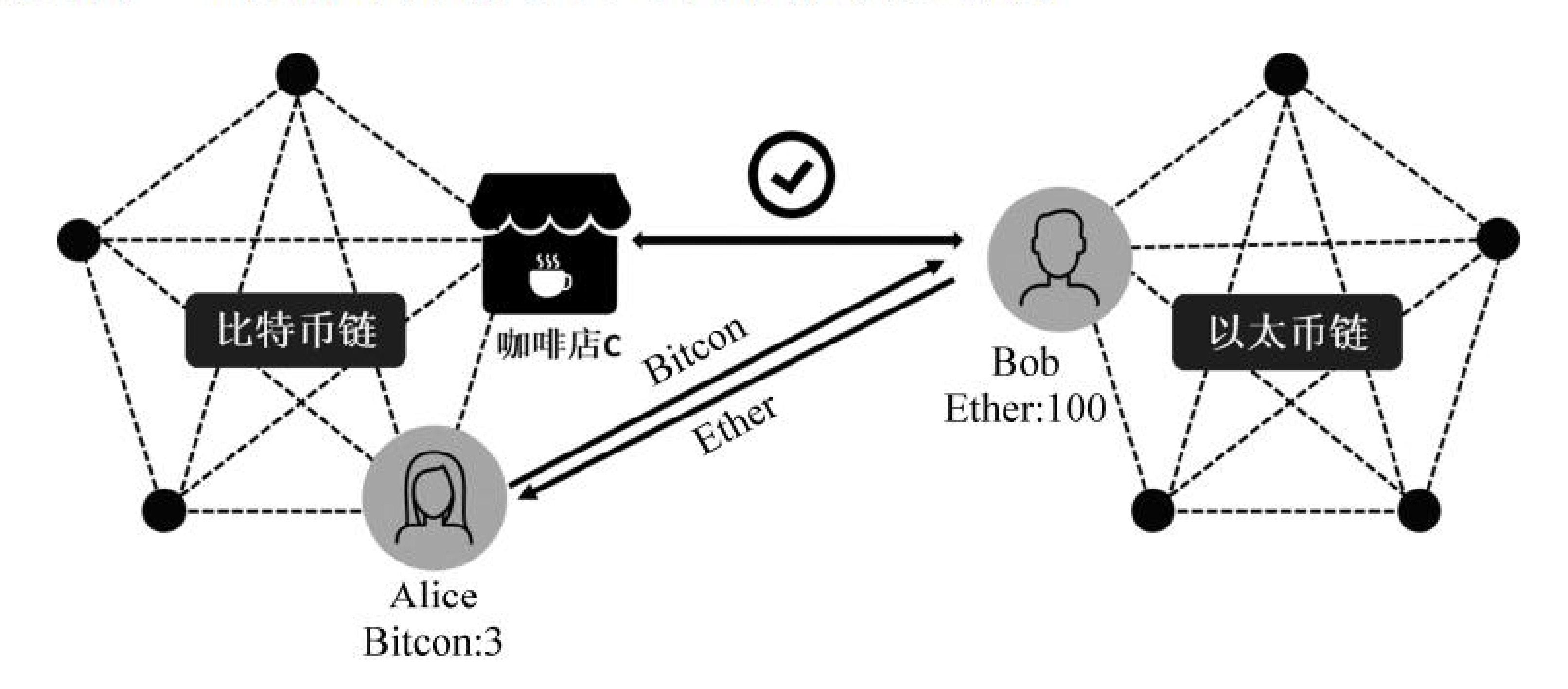


图 5.1　比特币网络与以太币网络跨链实例

Alice 是比特币的用户,持有 3 个比特币;Bob 是以太币的用户,持有 100 个以太币;咖啡店 C,支持比特币支付,且一杯咖啡的售价为 1 个比特币,但不支持以太币支付;Bob 通过跨链机制(比特币、以太币之间的跨链机制)从 Alice 手里兑换到一定比例的比特币,再使用比特币从咖啡店 C 买到了想要的咖啡,最终完成了使用自己持有的以太币从咖啡店购买一杯咖啡的交易。

对于跨链技术来讲,更为重要的应用领域是在区块链企业业务中。如果把区块链分布式账本类比于多家企业共同建立的一个分布式数据库,那每条区块链就相当于数据库中的一张数据表。对于复杂的企业业务场景,必然要采用多张表才完成业务。而每张数据表不可能都是孤立的,必然存在着一定的关联性、依赖性或者数据的一致性。以税收的场景为例,每个地域的企业可以与相关的税务部门组成一条区块链,记录纳税信息,但是,企业还会涉及采购、销售等上下游的相关企业,这些企业可能处于其他地域,这其中又涉及增值税数据的抵扣。所以,不同地域的区块链账本之间,数据存在一定的关联性和一致性。

跨链技术可以解决企业业务场景下的一个重要的问题——在保证业务协同性的情况下,尽可能地提升区块链系统的整体业务性能。通过跨链技术,将具有紧耦合的业务,放到一条区块链上,对于松耦合的业务,拆分到不同的链上,由跨链技术实现业务的协同和事务的一致性。

总体来说,当前的区块链系统都是相对独立的系统。不管是从性能上,还是从支撑的业务复杂度上,都已经成为区块链技术的发展瓶颈,必须要通过合适的跨链技术,实现区块链业务系统的互联互通和高性能。

当前设计与实现跨链的技术难点,主要集中于以下两方面。

(1) 交易验证问题:如何设计区块链系统之间的信任机制,使得一个区块链可以接收并且验证另一个区块链上的交易?

（2）事务管理问题：跨链交易包含多个子交易，这些子交易构成了一个事务，如何确定子交易是否被最终确认、永不回滚，及如何保证交易的原子性？所有子交易要么都成功，要么都失败。

5.3.2　常用解决方法

在多个区块链间进行跨链是一个复杂的过程，对于加密数字货币领域，有侧链、中继、哈希锁定等跨链实现方案，来完成数字资产的价值交换和转移。

1. 侧链

侧链是相对于主链而言的一个概念，它是以锚定某种原链上的代币为基础的新型区块链，正如比特币锚定到以太币。侧链概念的提出主要是为了实现比特币和其他数字资产在多个区块链间的转移。通俗地讲，侧链就是使区块链代币在不同区块链间转移的机制。侧链不像之前其他的区块链系统，对已有的区块链系统具有较强的排斥性，主链与侧链的关系如图 5.2 主链与侧链：

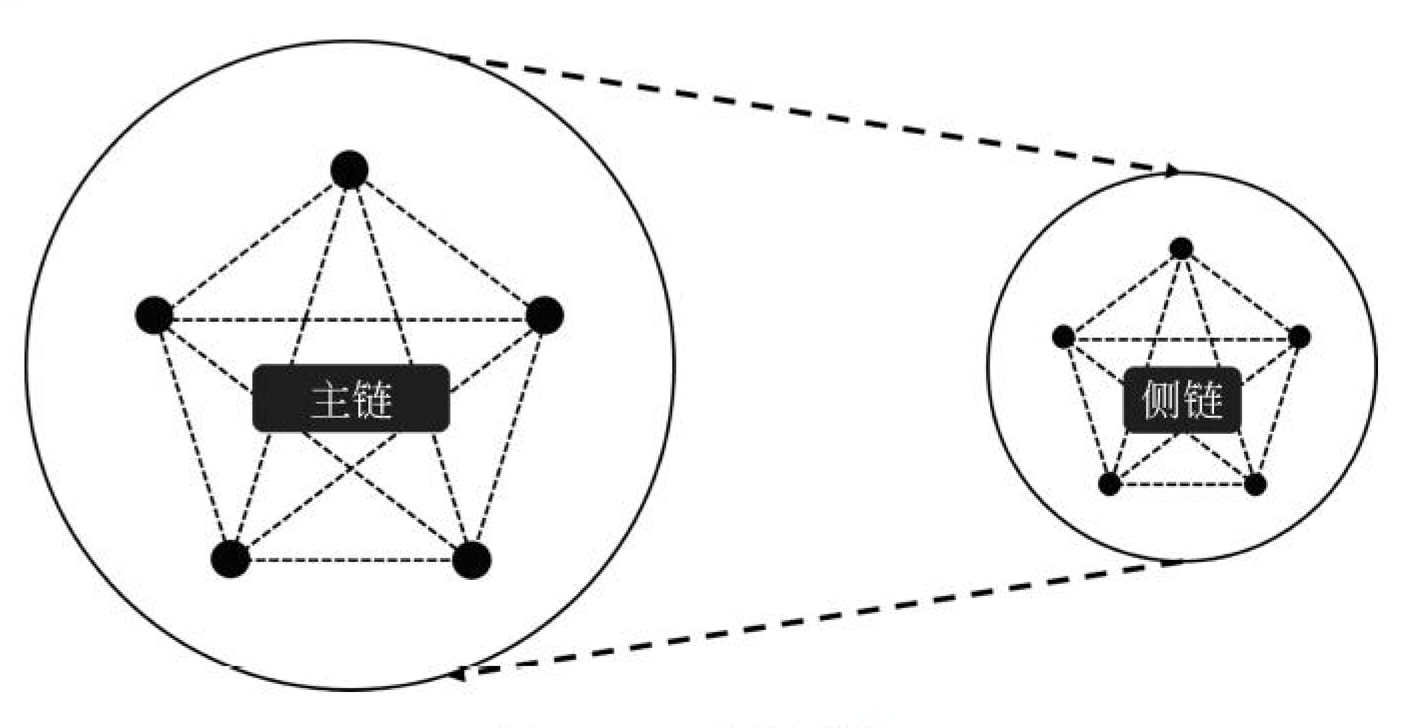


图 5.2　主链与侧链

如图 5.2 所示，可以将主链与侧链看成两个不同的系统，而虚线侧是数据流向，主、侧链的相互作用，可以简单地看作是两个系统间进行数据传输的过程。侧链的主要工作方式分为单一托管和合约联盟。当前的侧链系统中，有以下具有代表性的方案：

BTC-Relay，它是被认为区块链上的第一个侧链，主要原理是通过一种安全去中心化的方式把以太坊网络与比特币网络连接起来，BTC-Relay 基于以太坊的智能合约功能，使用户可以在以太坊网络上进行比特币交易。

Elements（元素链），作为比特币侧链，其最具创新意义的特性莫过于私密交易。私密交易中的金额仅由该交易的参与者知道（或其他指定的人可以知道）。比特币用地址来保证隐私，同时公开交易让别人验证。元素链在保护个人隐私上更进一步，因为其引入一种新地址类型，称为私密地址，私密地址含有一个盲化因子，因此比普通比特币地址更长，这种地址在元素链 Alpha 版本中是默认地址。

对于中继、哈希锁定等公链跨链技术，感兴趣的读者可自行网上查询。

对于在企业业务场景，应用更为广泛的区块链联盟链，还可以采用公证人机制实现跨链。

2. 公证人机制

这种模式相对简单,易于理解,和现实世界中的“公证人”很类似。假设 A 和 B 不是互相信任的,那就引入 A 和 B 都能够共同信任的第三方充当公证人作为中介。这样的话,A 和 B 就间接可以互相信任。此模式中,通过外部的公证人验证跨链消息的可靠性,公证人验证通过后必须对跨链消息签名。具有代表性的方案是瑞波实验室提出的跨链价值传输协议(Interledger Protocol,简称 ILP)。ILP 旨在连接不同账本并实现它们之间的协同。Interledger Protocol 适用于所有记账系统,能够包容所有记账系统的差异性,该协议的目标是要打造全球统一支付标准,创建统一的网络金融传输的协议。Interledger Protocol 使两个不同的记账系统可以通过第三方“连接器”或“验证器”互相自由地传输货币。记账系统无需信任“连接器”,因为该协议采用密码算法用连接器为这两个记账系统创建资金托管,当所有参与方对交易达成共识时,便可相互交易。

ILP 整个交易流程分成两个方向的流程:

(1) 由发送者向接收者;

(2) 由接收者向发送者。

每个流程又会由各自“账本”上的子交易组成,子交易包括托管创建和托管确认。

如图 5.3 所示,连接者同时处在发送者链上账本和接收者链上账本上,它与发送者通过发送者所在的链上账本进行交易,与接收者通过接收者链上账本进行交易。从发送者到接收者方向,会在所有账本上创建“托管”交易,“托管”交易在未被确认完成时,其交易内指定的资产转移不会真正发生。只有当接收者对“托管”交易确认完成后,从接受者向发送者方向上的各个“托管”交易才会被确认,此时所有账本上的“托管”交易才会被确认,各个“托管”交易内指定的资产才会真正转移。

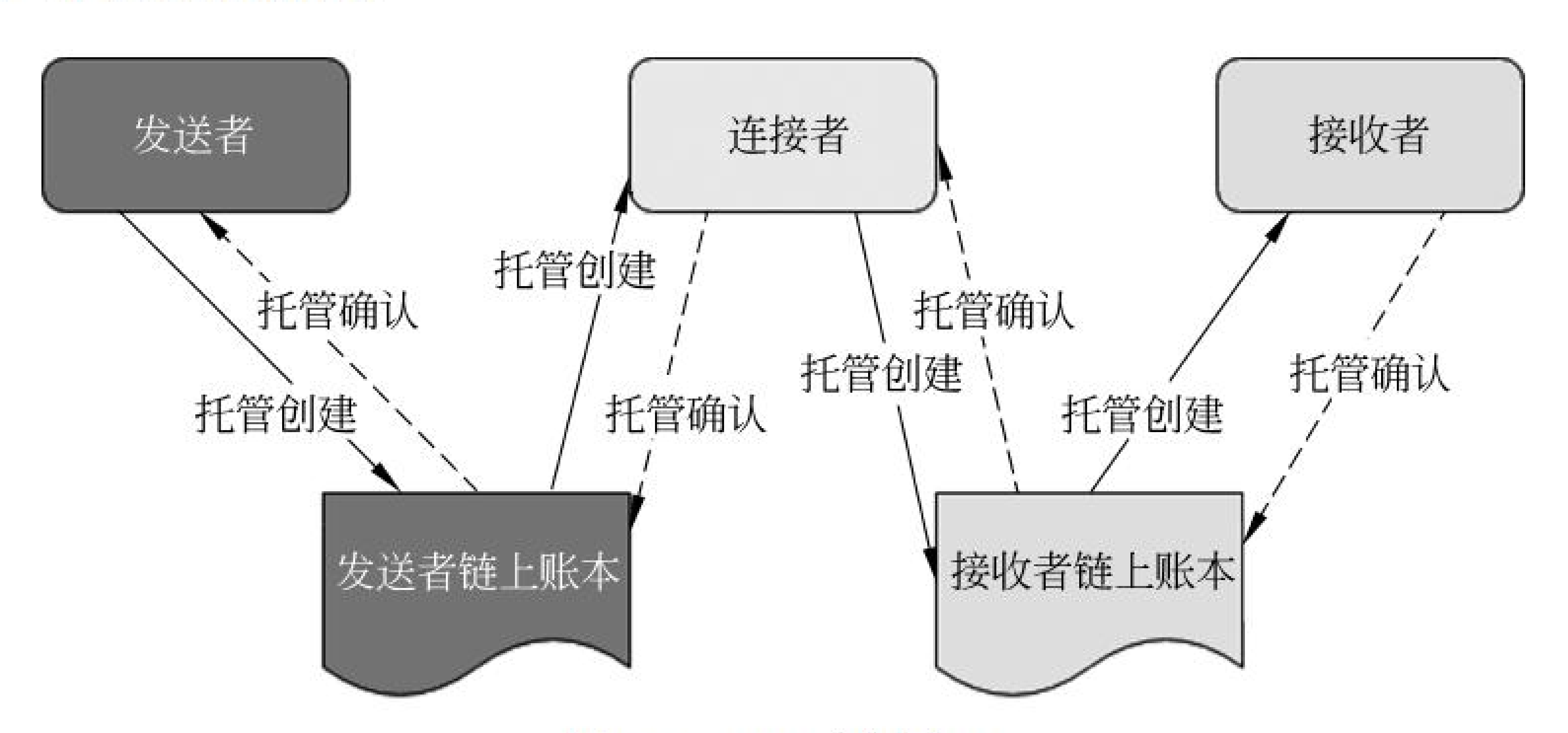


图 5.3 IPL 交易流程

而对于在企业业务场景中,应用广泛的区块链联盟链平台——Hyperledger Fabric,引入了通道的概念,它支持多通道并行运行,其中每个通道有一个独立的区块链账本,多个通道之间链结构相同,相互隔离,我们可以通过分布式事务技术,实现多条通道之间账本的协同和一致性。利用类似 Hyperledger Fabric 系统的水平扩容方案,将一个主链分成若干个同构的子链。

每一条子链的性能都是类似的。用户的业务可以承载在其中一条链上,通过跨链技术完成多业务之间的交互。系统的交易可以在多个子链上并行处理,达到了水平扩容的效果,从而使区块链系统的整体性能得到十倍甚至是百倍的提升。

5.4　图结构区块链

5.4.1　当前存在的问题

共识机制,是指由特殊节点对一个提议(在账本技术中很可能是包括了若干条交易的一个区块)进行投票,并完成对此提议的验证和确认的机制,通俗的说,对一笔交易的共识,就是由协同参与账本的几个节点达成一个一致的结果,如果达成否决的结果,则交易不记录进账本或者在账本中标记为无效,否则正常记录进账本。当前成熟的区块链共识机制主要是基于链式结构,如图 5.4 所示,主要的共识算法有:PoW、PoS、DPoS、PoI、PoP、PBFT 等。

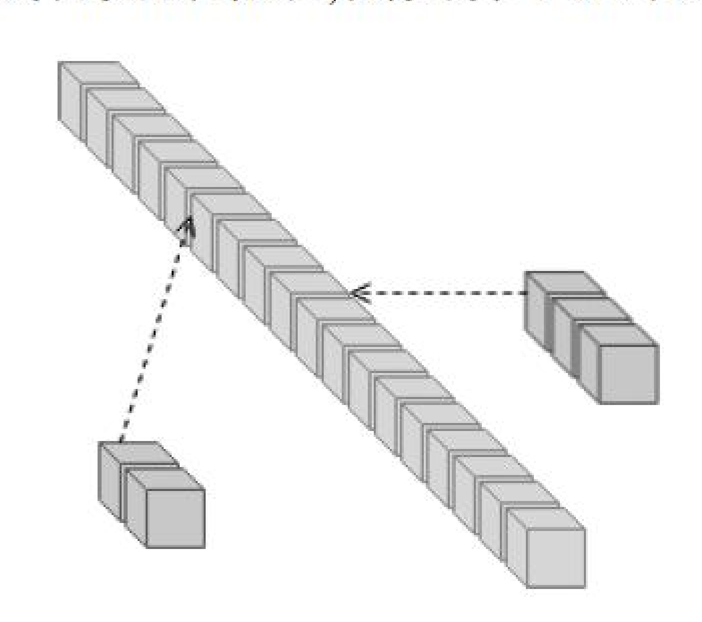


图 5.4　基于区块首尾相连结构的链

可以通过图 5.4 看到,基于以上共识算法产生的共识机制(结合链式结构),账本都会以单条链为准,好比有 5 家银行面向普通用户联合开放了一种特殊的优惠证券,不过购买时需要经过 5 家银行的信任评估,但是只开放了一个受理点,由于购买人数量较多,所有排队等待的人都需要经过漫长的等待,这个大大限制了办理的效率,同时信任评估需要五家银行现场连线确认,如果又有 3 家银行想要加入并提供信任评估,那么这个确认的时间也会随着新加入银行的数量而变大,可以看到基于链式结构的共识机制对于性能会有很大的限制,可以总结问题要点如下:

(1) 吞吐率低——在单位时间内可以完成确认的交易笔数较少,区块生成效率低下,不足以支撑现实场景中的高频交易,类似 VISA 信用卡交易;

(2) 共识节点扩容有限——尤其对于支持拜占庭容错的共识,节点数量过多时,将使得通信开销过大,从而极大地降低共识效率;

(3) 能耗大——这主要是针对类似 PoW 的共识机制,比拼算力最终演化成比拼电力。

5.4.2　常用解决方法

为了能攻克这些问题,业界有不少组织正在积极探索基于图结构的共识机制,更多时候,我们使用有向无环图(Directed Acyclic Graph,DAG),如图 5.5 所示。

有向无环图原本是计算机领域一种常用数据结构,因为独特的拓扑结构所带来的优异特性,经常被用于处理动态规划、导航中寻求最短路径、数据压缩等多种算法场景。而由于图结

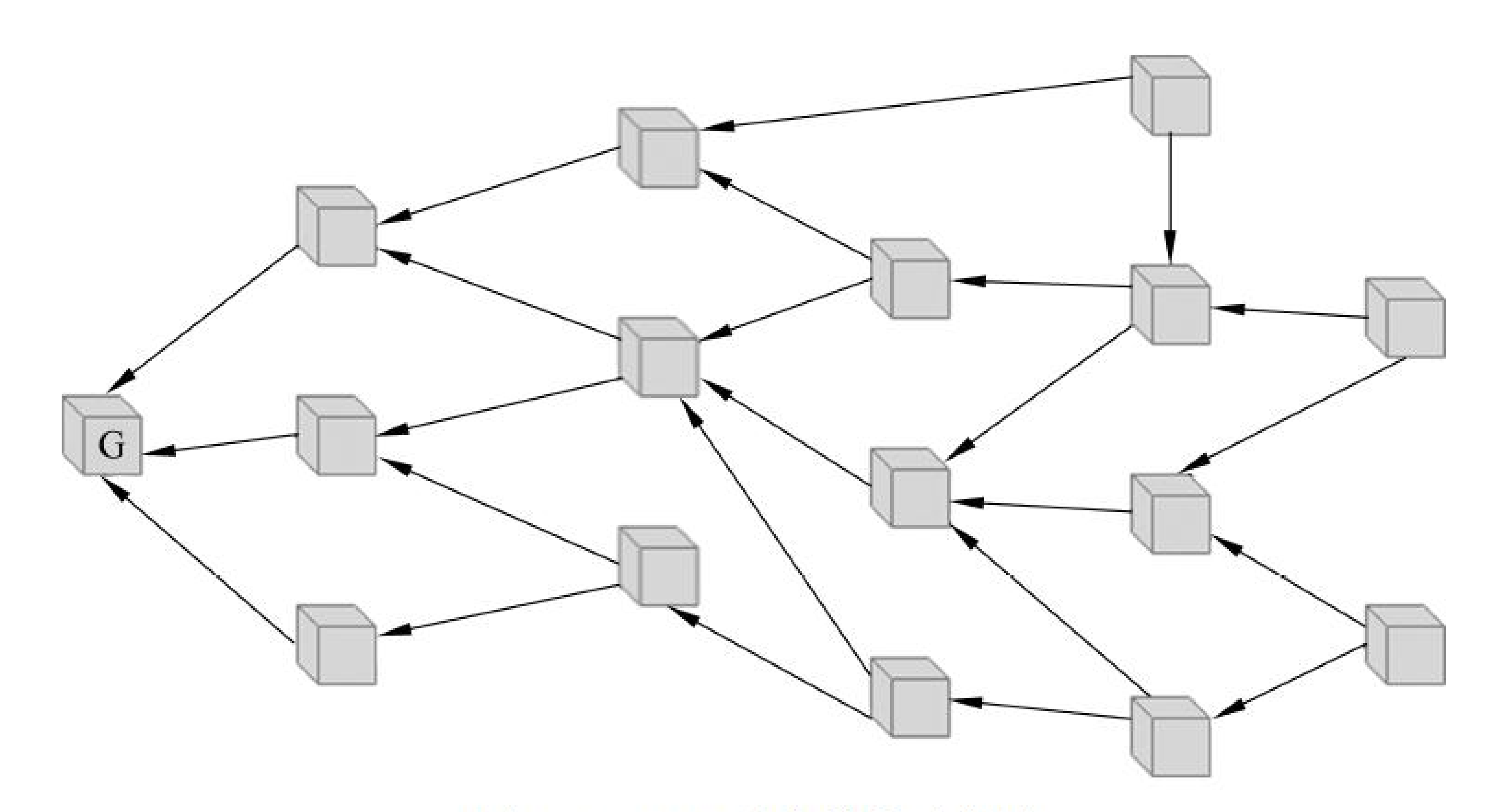


图 5.5 DAG 基本结构示意图

构比链式结构更益于区块的并行创建,所以普遍认为基于图结构的共识机制可以克服区块生成效率低下的问题。

传统区块链和图结构区块链的区别,简单地说是拓扑。区块链是由区块组成的单链,只能按出块时间同步依次写入,好比单核、单线程 CPU;图结构区块链是由交易单元组成的网络,可以异步并发写入交易,好比多核、多线程 CPU。当前较有代表性的图结构区块链的共识协议有:Tangle、Hashgraph、SPECTRE/PHANTOM 等。

1. Tangle

Tangle 是 IOTA 项目背后的共识协议,早在 2013 年就已经提出。协议概述:以交易来组织网络,一个节点发起新交易时,在 tangle 网络中找到 2 笔合法的历史交易作为父交易,并将自己的新交易指向这两笔交易作为子交易,指向的过程中也对父交易进行了验证。至于如何选取验证的父交易,Tangle 采用马尔可夫蒙特卡洛(Markov Chain Monte Carlo,MCMC)随机游走的方法,其目的是保证尽可能均匀地选出当前已记入账本的交易作为父交易,从而提升整体网络的确认度。同时,为提高产生交易的门槛,Tangle 中加入了交易的权重指标,由生成该交易完成的工作量决定交易权重的大小(如哈希值开头是几个 0 等),每个交易都具有累积权重,即该交易的权重加上所有直接、间接确认该交易的权重总和,代表着交易的确认度。另一方面,Tangle 给每个交易进行打分,其分数由该交易直接或间接确认的交易的总权重构成,并限定新交易只能确认分数达到一定标准的旧交易作为父交易,从而避免新交易过多选取过旧交易作为父交易的行为,保证网络的健康成长。

Tangle 的优势有如下几点:(1)由于新交易的加入较为轻量且方便,Tangle 网络中没有记账费用,对小额支付场景十分友好;(2)由于 Tangle 网络中交易相互确认的特性,使得该网络具有交易量越大,交易越快被确认的特点。

然而,Tangle 目前也存在一定的问题:(1)Tangle 中的共识是一种脆弱的共识,也就是随时间推移,交易确认度不一定上升;因此在整体 Tangle 网络中节点较少的当前,Tangle 放置了

一个闭源的协调者,该协调者发送 milestone 交易,并设定由该交易直接或间接确认的交易均为可信度 100% 的交易;然而,该协调者目前仍是中心化的实现,其降低了 Tangle 网络的去中心化程度;(2)Tangle 中的共识是由全网交易确定的,理论上讲,如果有人能够产生 1/3 的交易量,就可以将无效交易变成有效交易;(3)Tangle 网络中交易无手续费,所以没有矿工激励,其面临着拒绝服务攻击和垃圾信息攻击的可能。

2. Hashgraph

根据 Hashgraph 白皮书定义,其本质上是一种数据结构和共识算法,旨在解决异步拜占庭容错问题。根据 FLP 定理,在网络可靠且存在节点失效的异步分布式系统中,不存在一个可以解决一致性问题的确定性算法,可见 Hashgraph 也并非一个完美的异步拜占庭容错算法。Hashgraph 对确定性做了些许放宽,即在特定条件下,共识算法可能无法终止(即区块链中无法给出交易排序结果),但这种事件发生的概率极低,随着更多信息的汇入,共识算法无法终止的概率无限趋近于 0。Hashgraph 主要通过互相投票(Gossip about Gossip)以及虚拟投票(Virtual Voting)来实现共识过程,概述如下:

1)用事件记录交易,每个事件包括:交易、两个父节点的哈希值、时间戳、签名。

2)基于 gossip 协议,随机生长账本。通过 round 划分阶段,基于前后节点之间的连接关系确定每个阶段的 famous witness,再由 witness 确定 DAG 中的事件的顺序。

其特点在于:1)公平:账本具有一致的时间戳,可以对每笔交易进行定序;2)安全:其所使用的异步拜占庭容错(Asynchronous Byzantine Fault Tolerance,ABFT)系统,有相当的安全理论证明,验证简单;3)速度快:可达到 250 000TPS 的吞吐量。

Hashgraph 当前存在的问题主要包括:1)gossip 算法在大规模公链环境下的应用可能会遇到问题;2)其中的每个共识节点均需要保存全网数据,数据压缩问题不易解决。

3. SPECTRE/PHANTOM

SPECTRE 和 PHANTOM 是由 DAGLabs 公司推出的基于 DAG 结构的区块链扩容共识协议。DAGlabs 是一家位于美国加州旧金山的区块链技术服务公司。主创人员包括了 SPECTRE 和 PHANTOM 的联合作者 Yonatan Sompolinsky 和 SPECTRE 的联合作者 Yoad Lewenberg。SPECTRE Protocol 采用了 BlockDAG 的技术,可以并行挖矿,从而带来更大的吞吐量和更快的交易确认时间。2018 年 2 月基于 SPECTRE 改进的扩容协议 PHANTOM 发布,能够大大扩充网络交易容量,并兼容智能合约。不同于闪电网络等链下解决方案,PHANTOM 是链上扩容方案。PHANTOM 主要通过使用具体偏序变全序的算法来确定整个 DAG 上区块的线性排列,从而达到对整个 DAG 组织里的区块的共识。虽然 PHANTOM 实现了区块在 DAG 上的线性排列,并大大提高了整个网络的交易容量,但它并不保证迅速地确认区块时间。

凡事都有两面性,DAG 的结构天然支持了区块的并行创建,让人有直观的感觉,可以轻松地提升吞吐量。但基于 DAG 结构的共识协议,一致性未得到有效的验证和认可,同时应用场景也不同于传统区块链那么广泛;但 DAG 结构的优势和基于 DAG 结构的共识创新已经慢慢

出现到人们的视野之中,相信不久的将来,会有越来越多基于 DAG 结构的创新项目、共识机制会成熟地出现到各类应用之中。结构的创新项目、共识机制会成熟地出现到各类应用之中。

虽然当前基于 DAG 结构的共识机制还未完全解决以上所述问题,我们可以适当保持理性的态度,将其视为区块链技术的一个必然的探索方向,大胆地去尝试,大胆地去创新。

5.5 本章小结

目前的区块链技术尚处于发展的初级阶段,在技术层面上仍存在许多问题。本章主要从两个方面来讲述区块链的发展趋势,分别是当前存在的问题以及解决问题的思路。第一个趋势是隐私保护,由于有许多领域的数据是不适合公开的,因此目前这种完全公开透明的区块链就需要被改进。目前主要的解决方案有同态加密、零知识证明以及利用可信执行环境等。第二个趋势是跨链交易。区块链作为一种价值网络,必然会需要在不同的链之间进行价值交换,因此跨链交易就显得尤为必要。目前的解决方案有侧链和公证人机制。第三个趋势是图结构的区块“链”。由于目前的区块链技术存在一定程度的扩展性问题,人们开始考虑区块链并不一定要是一个链状结构。有向无环图作为一种常用的数据结构,被一些研究人员借鉴来替代区块链的链状结构,目前已有的实现有 Tangle、SPECTRE 和 HashGraph 等。本章能够帮助读者深入地思考未来区块链的发展趋势,把握区块链的创新潜力。



第二部分 区块链应用

随着区块链技术的逐步发展,其应用潜力正得到越来越多行业的认可。从最初的加密数字货币到金融领域的跨境清算,再到供应链、政务、数字版权、能源等领域,甚至已经有初创公司在探索基于区块链的电子商务、社交、共享经济等应用。只要涉及多方协同、不存在一个可信中心的场景,区块链均有用武之地。当前区块链应用处于发展初期,主流的区块链应用均是利用了区块链的特性在原有业务模式下进行的改进式创新,区块链作为从协议层面解决价值传递的技术理应有更广阔的应用场景。我们有理由相信下一个基于区块链技术的“爆款”应用将带来巨大的模式创新,并将颠覆原有的产业模式。

第6章 区块链应用的价值和场景

比特币作为区块链技术的第一个应用,其出现为区块链技术在众多领域的使用和推广拉开了序幕。从最初的加密数字货币到后来的金融应用,再到近年来在各大行业领域的广泛使用,区块链技术正以其独特的价值深入影响和改变人们的认知与生活。

从图6.1中我们可以看到,区块链具体应用领域在不断扩展,而这正是由于我们对区块链的认识和理解不断深入而逐步发展的。最初我们只是片面地认为区块链只用于虚拟货币交易,然而随着对其链式结构原理和不可篡改等特性的了解,我们惊喜地发现区块链适用的交易其实不只局限于货币,一切金融界的交易都可以用区块链来记录。紧接着随着我们对区

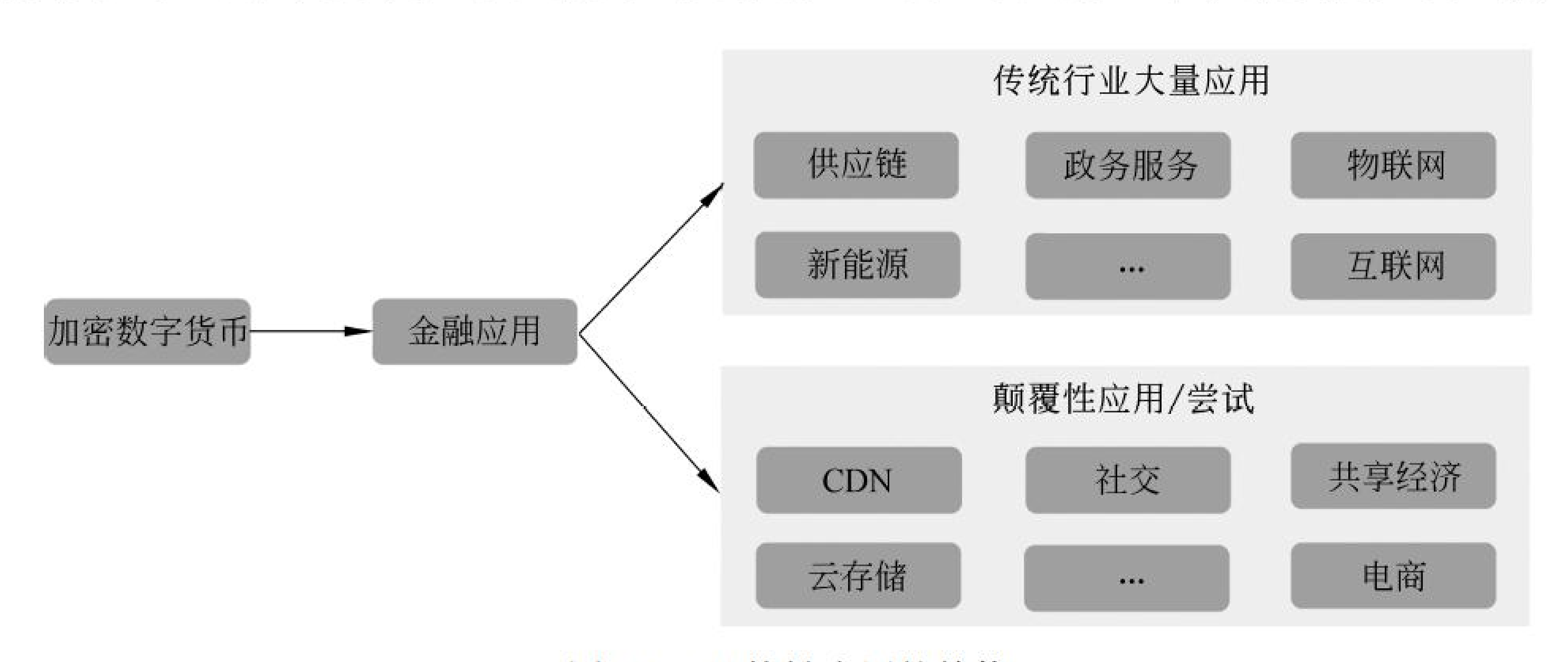


图6.1 区块链应用的趋势

块链传递信任本质的领悟,大家恍然大悟,需要传递信任的地方就需要区块链,金融业只是区块链应用场景的一个分支。由此区块链的应用领域一下被扩展到各种行业:供应链、政务服务、物联网、新能源,甚至庞大的互联网也只能说是区块链领域的一个分支。我们更相信随着区块链应用领域的不断拓展、区块链应用规模的不断扩大,未来将会催生出大量的以区块链为创新点的颠覆性应用,我们的社会也由此向着可信社会的方向迈进。

6.1 区块链应用的价值

区块链提供一种在不可信环境中,进行信息与价值传递交换的机制,是构建未来价值互联网的基石,也符合我国十九大以来一直提倡的为实体经济提供可信平台。区块链发展到现在,我们可以从以下几个方面来分析其应用的方向:

- 从应用需求视角可以看到,区块链行业应用正加速推进。金融、医疗、数据存证/交易、物联网设备身份认证、供应链等都可以看到区块链的应用。娱乐、创意、文旅、软件开发等也有区块链的尝试。
- 从市场应用来看,区块链也逐步成为市场的一种工具,主要作用是减少中间环节,让传统的或者高成本的中间机构成为过去进而降低流通成本。企业应用是区块链的主战场,具有安全准入控制机制的联盟链和私有链将成为主趋势。区块链也将促进公司现有业务模式重心的转移,有望加速公司的发展。同时,新型分布式协作公司也能以更快的方式融入商业体系。
- 从底层技术来讲,有望推进数据记录、数据传播和数据存储管理模式的转型。区块链本身更像一种互联网底层的开源协议,在不远的将来会触动甚至会最后取代现有的互联网底层的基础协议(建筑在现有互联网底层之上,一个新的中间层,提供可信的有宿主的有价值的数据)。把信任机制加到这种协议里,将会是一个很重大的创新。在区块链应用安全方面,区块链安全问题日渐凸显,安全防卫需要技术和管理全局考虑,安全可信是区块链的核心要求,标准规范性日显重要。
- 从服务提供形式来看,云的开放性和云资源的易获得性,决定了公有云平台是当前区块链创新的最佳载体,利用云平台让基于区块链的应用快速进入市场,获得先发优势。区块链与云计算的结合越发紧密,有望成为公共信用的基础设施。
- 从社会结构来看,区块链技术有望将法律、经济、信息系统融为一体,颠覆原有社会的监管和治理模式,组织形态也会因此发生一定的变化。虽然区块链技术与监管存在冲突,但矛盾有望进一步调和,最终会成为引领人们走向基于合约的法治社会的工具之一。

什么领域适合区块链技术?我们认为在现阶段适合的场景有三个特征:第一,存在去中心化、多方参与和写入数据需求;第二,对数据真实性要求高;第三,存在初始情况下相互不信任的多个参与者建立分布式信任的需求。

典型的应用案例如：华为物流部基于区块链进行货物跟踪，该区块链应用提升了数据安全性、隐私性、共享性，解决了商品转移过程中的追溯防伪问题，有效提高物流行业在结算处理效率，节约 20% 以上物流成本；基于华为云区块链所打造的供应链金融平台，该平台加强了供应链金融业务中多方信息的共享，简化企业间的互担保、风险分摊、机构信用评估等流程，提升企业融资效率，融资过程从半个月降低到 2 天，同时也降低违约处理成本；基于华为云区块链实现数据内容版权区块链平台，数据内容版权公司能够为海量作品提供低成本、高效率的版权存证方案，版权存证处理流程耗时由 10 – 20 天提升到实时版权存证，促进版权合理合法的快速流通。

区块链应用的发展趋势如图 6.1 所示，从比特币加密数字货币，到金融结算市场的优化，逐渐演进到创造性地重构传统行业的大量应用如供应链金融、供应链溯源、新能源交易系统、物联网等。随着应用场景日益丰富，应用将推动着区块链技术不断完善，区块链与云的结合日趋紧密，该技术也会逐渐地应用于新兴市场经济如房屋租赁共享经济、社交网络、内容分发网络等场景中。区块链系统以其特有的价值实现在数据流转过程中不可逆，从而保障数据的可靠性；区块链数据流转的可信性，将有效简化流程、提升效率、降低成本；区块链的系统架构和优势使构建产业生态更加容易并降低产业成本。可以预见，区块链是价值网络的基础，将逐渐成为未来互联网不可或缺的一部分，区块链技术也将逐步适应监管政策要求，逐步成为科技监管领域的重要组成部分。

6.2　区块链应用场景

高盛在 2016 年发布的一份区块链产业报告中指出，区块链独特的性质使得它不仅有潜力优化现有市场，也有能力重构市场和创造新市场，具体包括以下几点：

- 在创造新市场方面，其代表案例如个体家庭住宿的兴起，至 2020 年，30 亿 ~ 90 亿美元的新生市场订房费用增量，区块链可以安全地储存和整合用户的在线交易信息，并检查身份验证和支付认证的历史记录，使得各方建立信任更加容易。
- 在创造性地重构市场方面，其代表案例如智能电网的分布式售电系统，会带来价值 25 亿 ~ 70 亿美元的美国分布式能源市场，区块链可以连接本地的能源生产者（比如有太阳能板的邻居）与该地区的消费者，使得分布式的实时能源交易市场成为可能。
- 针对优化现有市场，代表案例如金融结算场景，采用区块链系统可以显著缩短交易的结算时间，甚至是从几天缩减到数小时，这也可以帮助减少全流程的资本需求、运营成本和托管费用，实现每年全球 110 亿 ~ 120 亿美元的成本节约。

在未来 5 ~ 10 年，区块链有可能触及很多行业，最可能产生颠覆性的行业包括金融业、共享经济和社交网络、存储和内容分发网络等。

首先在金融业领域，区块链为金融机构系统性地解决全业务链的痛点和顽疾。区块链技术可以被应用在不同的银行业务，从支付结算、票据流转、供应链金融、到更复杂的证券发行与交易等各核心业务领域。区块链技术带来的收益将惠及所有的交易参与方，包括银行、银

行客户、银行的合作方(如平台企业等)。目前金融服务各流程环节存在效率瓶颈、交易时滞、欺诈和操作风险等痛点,大多数有望在区块链技术应用后得到解决,规避现有流程中大量存在的手工操作。比如区块链技术的应用可以帮助跨境支付与结算业务交易参与方节省约40%的交易成本。金融业典型的应用场景包括:

- 数字货币:随着电子金融及电子商务的崛起,数字货币安全、便利、低交易成本的独特性,更适合基于网络的商业行为,将来有可能取代纸质货币的流通,中国央行也在研究法定数字货币,用以提高货币发行、使用及调控的便利性,区块链技术是可能的底层技术之一。
- 跨境支付与结算:区块链将摒弃中转银行的角色,实现点到点快速且成本低廉的跨境支付。通过区块链的平台,不但可以绕过中转银行,减少中转费用,还因为区块链安全、透明、低风险的特性,提高了跨境汇款的安全性,以及加快结算与清算速度,极大提高资金利用率。
- 票据与供应链金融业务:借助区块链的技术,可以直接实现点对点之间的价值传递,不需要特定的实物票据或是中心系统进行控制和验证;传统中介的角色将被消除,也减少人为操作因素的介入。供应链金融也能通过区块链减少人工成本、降低成本及操作风险、提高安全度及实现端到端的透明化。
- 证券发行与交易:区块链技术使得金融交易市场的参与者享用平等的数据来源,让交易流程更加公开、透明、有效率。通过共享的网络系统参与证券交易,使得原本高度依赖中介的传统交易模式变为分散的平面网络交易模式,实现准实时资产转移,加速交易清算速度。
- 客户征信与反欺诈:记载于区块链中的客户信息与交易记录有助于银行识别异常交易并有效防止欺诈。区块链的技术特性可以改变现有的征信体系,降低法律合规成本,防止金融犯罪。在银行进行客户身份识别(Know Your Customer,KYC)时,将客户的数据储存在区块链中。客户信息及交易记录不仅可以随时更新,同时,在客户信息保护法规的框架下,如果能实现客户信息和交易记录的自动化加密关联共享,银行之间能省去许多KYC的重复工作。

在共享经济和社交网络应用中,区块链天生就具备去中心化的特性,这一点与共享经济的宗旨高度吻合。区块链作为一个去中心化的一致性共享数据账本,在此架构下,整个系统的运作都是公开透明的,它将让共享经济变得更加容易。比如可以将智能合约运用于自行车租赁、房屋共享等领域,如果这种智能合约运用于今天火爆的共享单车领域,也许会给整个行业带来全新的改变,国外企业在此领域基于区块链技术做了如下的尝试:

- Synereo社交网络是基于加密、去中心化和点对点的网络平台,无需中央服务器,这意味着信息不会被阻挡或者被窃取。相反,Synereo平台由大量分散的节点支撑,由用户来运营,跟比特币的运作方式很相近。这就是说没有中心化实体能监视用户的行为,删除发帖,包括Synereo自己。用户只要能够连接网络,就可以加入这个社交网络。

发帖并不暴露用户身份。如何平衡政府监管和用户隐私保护是该系统商业成功与否的非常关键的因素。

- Slock. it 致力于发展共享经济的未来基础设施。我们将其称为通用共享网络(USN)。依托于公共以太坊区块链,通用共享网络将为用户提供一套可移动的桌面应用程序,通过它们,用户可以从世界任何地方找到、定位、租赁和调控由智能合同介导的对象。
- OpenBazaar 是一个结合了 eBay 与 BitTorrent 特点的去中心化商品交易市场,相对于易趣与亚马逊这些提供中心化服务的电子商务平台,通过 OpenBazaar 不需要支付高额费用、不需要担心平台收集个人信息导致个人信息泄露或被转卖用作其他用途。

在存储和内容分发网络(Content Delivery Network,CDN)领域,传统型和云服务型厂商受限于昂贵的 CDN 基建成本,其 CDN 加速节点往往只能在大城市布点。如果这种大型节点遭受攻击,受影响的是千千万万的用户。而区块链 + CDN,按照每个区块链硬件用户都成为一个加速节点的实际情况,加速节点是无限的,同时安全性能随节点数增加而无限叠加,这是因为区块链技术特有的分布式计算保证了无论是任意一个节点,乃至成千上万个节点同时遭受攻击,剩余的节点数据都能无限期储存,面对这样一个滴水不漏的全覆盖网络,可以大幅度地提升抵御攻击的能力。已经有 CDN 服务供应商在该领域做尝试,共享者通过共享家庭闲置带宽和存储,获得激励,而 CDN 服务供应商通过共享者提供的资源获得大量的廉价带宽和存储,给用户提供有竞争力的 CDN 服务。

6.3 区块链应用潜力

在区块链目前已有的落地场景中,大多数是现有业务的改进,远没有发挥区块链的潜在威力。前沿的研究认为区块链会催生一种自组织商业模式的兴起,即以区块链为基础架构,以人工智能为驱动引擎,让相同层次趋同利益对等诉求的相似/互补的人聚合到一起,安全透明的交互,形成新的商业生态。

区块链在金融产业以主角现身,在以后的发展中,区块链更有可能隐身到幕后。如果说互联网是信息的高速公路,区块链就是价值的安全航线和可信的价值互联网。它从网上无序混乱、真伪难辨的数据中提取有潜在价值的部分,以拥有者的信用作背书,在完成共识后,实现并放大价值。在整个过程中,区块链是互联网和应用(智能合同)的连接层,向下屏蔽垃圾数据,向上输送可信行为。

在新型的自组织模式中,人工智能是搜寻者的角色,它在 A 需要一个人时,就把 B 送到 A 跟前,而 B 正是 A 所寻找的那一个。一些创业公司正在探索这种模式。

一个例子来自健康行业。穿戴设备的兴起让人体的真实数据有了可靠的医用价值,个人数据成为一种资产,可以授权,可以转卖。而医疗研究机构急需这样的数据。如果双方能够找到合适的结合点,医用数据的爆发有助于让保健部分代替医疗。

还有创意娱乐业的实践。内容提供者把自己的创作定向发布,获取打赏。作品在打赏中

升值,进入更大的传播空间,而观众也可以自由选择。

6.4　本章小结

本章从加密数字货币到金融领域,逐渐扩展到需要传递和建立信任的各个领域阐述了区块链应用的发展趋势,并从应用、市场、底层技术、服务提供形式、社会结构等方面分析了区块链应用的发展方向。本节论述了适合区块链场景的三个特征即去中心化多方参与、对数据真实性要求高、需要逐渐建立多方信任关系。此后本章基于高盛区块链产业报告,进一步阐述了在优化现有市场、重构市场和创造新市场的分类中典型的区块链应用的案例。

第7章 金融应用案例

在区块链应用领域,金融行业一直是最活跃的地方,常见的场景如跨境清算、中小微企业的贸易融资、银行客户身份识别。中国人民银行原行长周小川曾表示:“央行认为科技的发展可能对未来支付业务造成巨大改变,央行高度鼓励金融科技发展。数字资产、区块链等技术会产生不容易预测到的影响。在发展过程中出现的问题,需要进行规范。”

随着区块链技术的发展,包括中国央行、摩根大通、汇丰银行等众多顶级金融机构都开展了丰富的研究与试验性落地。相比传统的金融行业,更能够从安全、效率、互信建立等方面带来优秀的解决方案,本文通过以下几个场景来进行阐述。

7.1 区块链在跨境清算场景中的应用

7.1.1 业务场景

商业银行开展跨境结算业务有两种操作模式,即代理模式和清算模式。所谓代理模式,主要是指中资行委托外资行作为其海外的代理行,境外企业在中资企业的委托行开设人民币账户的模式;而清算模式主要是在指在中资行境内总行和境外分支行之间进行的业务,即境外企业在中资行境外分行开设人民币账户。

——摘选自百度百科

在跨境清算场景中,平时用户可见的流程仅为:前往金融机构填写申请表并支付费用,等

待对方收到账目。但是其实中间有一串冗长的流程,如图 7.1 所示,即从汇款人开始汇款、汇款行账户行 、各币种清算系统、收款行账户行、收款行和收款人,途中经历了 5 个环节。每个环节中还要经历 3 – 5 个小环节,大量的中介机构参与其中,一笔 10 000 美元的汇款大概 2 – 3 日才能到账。



图 7.1 传统跨境交易模式

7.1.2 行业现状和业务痛点

目前传统的跨境支付主要是采用传统的 SWIFT 网络完成,但是在每一个衔接的环节仍然需要大量的人工核查,传统 SWIFT 业务系统本身成本高、耗时长。在 KYC 过程中,不同的金融机构对客户信息的真实性控制有限,也会遇到共享的安全问题。主流的代理模式为了保证交易的准确性,需要实现全流程逐个机构、逐笔交易的信息确认,导致效率低,差错率高。

可见跨境清算存在效率低、成本高、交易不透明等痛点。区块链与跨境支付的结合,利用区块链去中心、分布式账本特点,实现点对点交易。打通中间环节、构建可信交易,最大限度提升效率,节省成本开支,如图 7.2 所示。

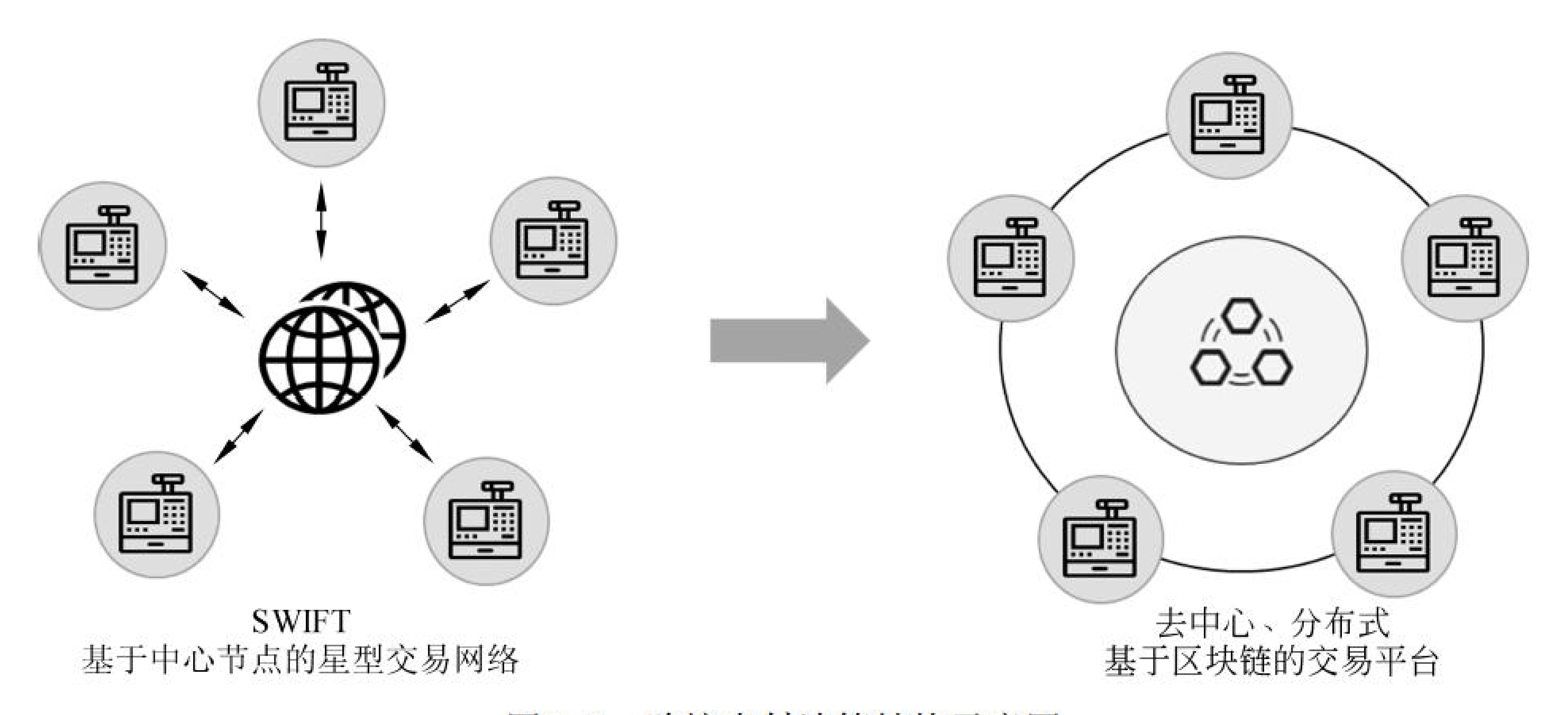


图 7.2 跨境支付清算结构示意图

7.1.3 基于区块链的解决方案

基于区块链平台的银行清算是网状结构。整个网络有多个节点中心,每个参与者(节点)都是权利和义务均等的个体,依靠所有参与者之间的相互约束建立信任。每个参与者都会记

录这个区块链上发生的所有清算交易数据，具有不可抵赖性。交易信息也可经过加密处理，只有交易相关角色方可解密。另外，监管方也参与到区块链的网络中。目前监管对银行来说是非常重要又头疼的角色。一方面需要维持金融秩序，另外一方面需要配合监管提供大量的文件和材料。如果监管也能成为清算环节中可随时获取信息的角色，那么监管就可以保存全量数据，并拥有查看每一笔交易以及参与者管理的权限，极大提高了监管的效率。

我们以招商银行实现的跨境支付清算为例：招商银行作为代理清算行，完成从香港永隆银行向永隆银行深圳分行的人民币头寸调拨业务。三方又完成了以招商海通贸易有限公司为汇款人，前海蛇口自贸区内海通（深圳）贸易有限公司为收款人的跨境人民币汇款业务。通过总行与海外分行间的直联通道，实现快捷便利的跨境支付功能，采取日间垫付、日终双边差额清算的模式。招商银行通过区块链平台进行点对点跨境支付，实现跨行跨境高效清算，提升资本运转效率，交易时间从一周降低为2小时。

区块链为基础的跨境支付，需要所有参与环节全部加入支付链中，交易各方不再依赖一个中心化的系统，用户可以实时的查看资金的流向，在这个过程中节省的不仅是人力、时间成本，用户体验也大幅提升。

与此同时，各大银行也积极地开展区块链相关业务的验证与开发，如工商银行基于区块链的点对点金融资产转移和交易服务，江苏银行区块链积极开展微众银行的联合贷款、银行微粒贷联合贷款的结算和清算等。

在贸易金融融资场景中，区块链可以发挥用户网络效应和应用协同效应。贸易金融业务的特点是规模大、场景庞杂、参与者众、难以用一个系统或一个机构服务所有客户和全部场景，因此传统上采用“分而治之”的方式建设系统，这就带来了一个问题：不管是按照行业划分还是按照业务类型划分，都很难最大化地发挥用户的网络效应以及场景的协同效应。而区块链技术的应用，则可以让平台尽可能承载更多业务场景，在同一个平台实现数据、用户的统一，使不同业务场景可在同一个平台上实现交互协同，从而发挥网络效应和协同效应。区块链可以整合更多的数据源和政府资源。贸易金融业务是一个社会系统工程。它的顺利开展离不开政府部门（工商、税务、海关、法院、交通等）以及众多贸易服务商的参与。这就涉及各方数据传输和资源整合的问题。区块链技术为贸易金融平台提供了一个更为灵活、开放的系统架构。基于区块链技术的贸易金融平台能够很好地解决传统上依靠人工，业务效率低，融资成本高，重复融资、虚假融资风险大等贸易金融难题。

区块链金融服务还可以延伸到传统业务难以覆盖的边远地区。例如，小额汇兑因为交易费用低不被重视，利用手机加上区块链技术是解决这个问题的可行方法之一。

7.2　区块链在供应链金融场景中的应用

7.2.1　业务场景

供应链金融是贸易金融的一个典型场景，如图7.3所示，它是指在供应链的业务流程中，

以核心企业为依托,运用自偿性贸易融资的方式,对上下游企业提供综合性金融产品和服务,整个行业在全球占据级万亿级的市场。举个简单的例子来说明供应链金融,一家企业和供应商A签订采购合同,金额为1000万元,合同在12个月后到期,当然合同款也是在12个月后才能付清,然而供货的生产需要600万元的资金,传统金融思路是供应商不得不想办法去金融机构贷款,并支付高额的利息,从而间接增加了生产成本,同时金融机构一方放款可能并不及时,放款金额也和该供应商的资质、信用甚至是抵押物有关。供应链金融就是试图使用新的方式来解决过程中各方的金融需求,比如将业务过程中的采购合同作为抵押物,金融机构校验合同真实性后就可以和供应商A签订贷款合同,同时提前放款600万元给供应商,12个月采购合同到期后,企业直接付600万元的本金和相应利息给金融机构,剩余的钱直接付款给供应商A,因此银行的风险极大降低。

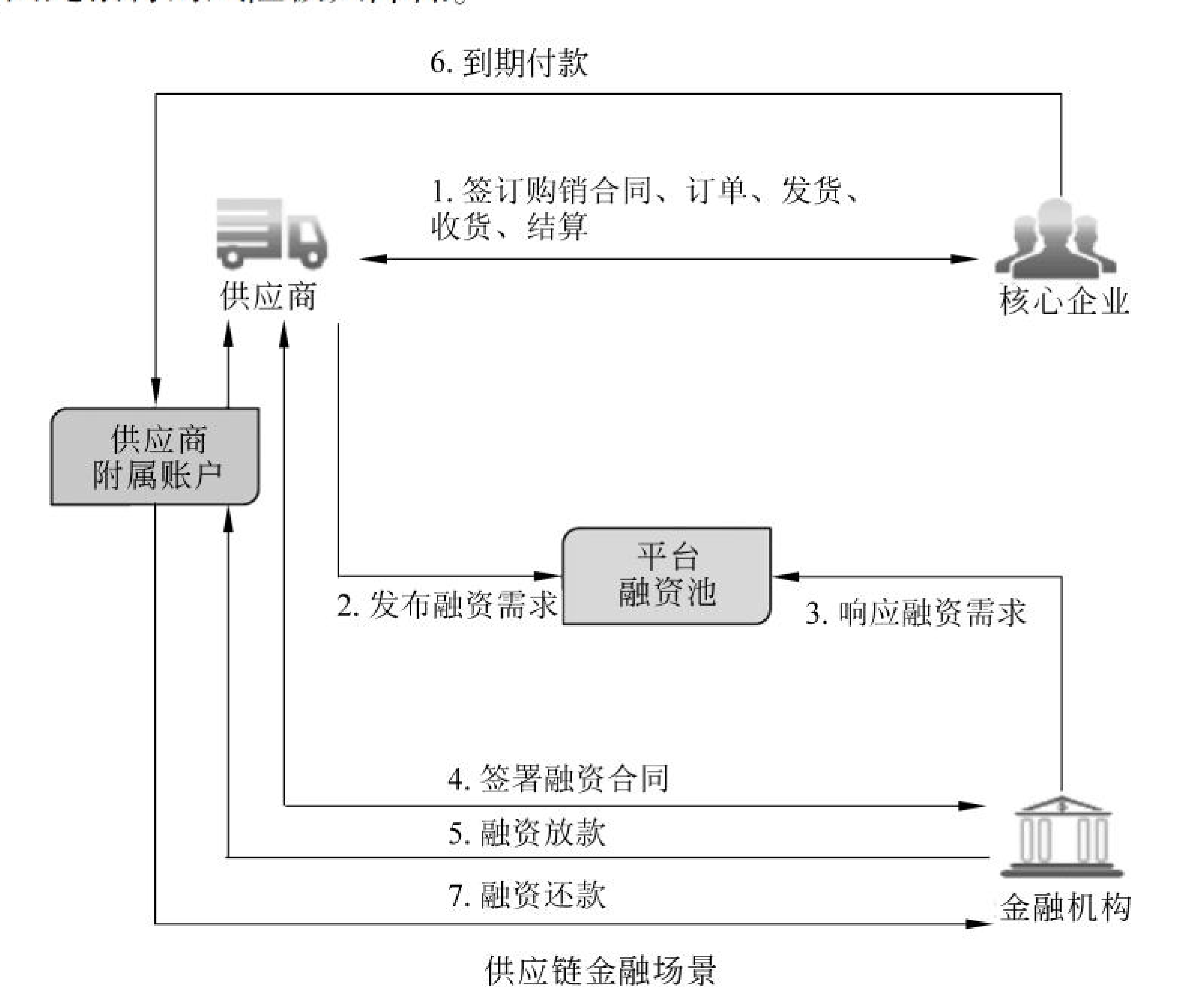


图7.3 供应链金融场景

7.2.2 行业现状和业务痛点

从例子中我们看到这是一个三赢的局面,企业和供应商的业务可以正常开展,金融机构也从中受益,所以供应链金融思路的核心就是打通传统供应链中的不通畅点,让业务流中的资金都可以顺利地流动起来。当然其中的过程有很多关键点,比如合同是否真实,合同额有没有被非法的篡改,企业有没有不诚信记录,合同到期后企业能否按时顺利的付款等。

另外,在现行金融贸易领域中,存在高成本的人工核查、众多银行之间的信息不流通、监管难度大、中小企业申请银行融资的成本高等问题。银行在为客户办理业务时,通常通过人

工的方式进行情报资料收集、信息对比验证、现场实地考察和监督,来了解客户情况和贸易背景,开展业务风险控制以及管理。

供应链金融领域目前的难点有如下几点:

首先,高度依赖人工的交叉核查,即银行须花费大量时间和人工判定各种纸质贸易单据的真实性和准确性,且纸质贸易单据的传递或差错会延迟货物的转移以及资金的收付,造成业务的高度不确定性;其次,金融贸易生态链涉及多个参与者,单个参与者都只能获得部分的交易信息、物流信息和资金流信息,信息透明度不高;再次,资金管理监管难度大,由于银行间信息互不联通,监管数据获取滞后,例如不法企业"钻空子",以同一单据重复融资,或虚构交易背景和物权凭证;四是中小微企业申请金融融资成本高。由于以上几个难点,为了保证贸易融资自偿性,银行往往要求企业缴纳保证金,或提供抵押、质押、担保等,因此提高了中小微企业的融资门槛,增加了融资成本。

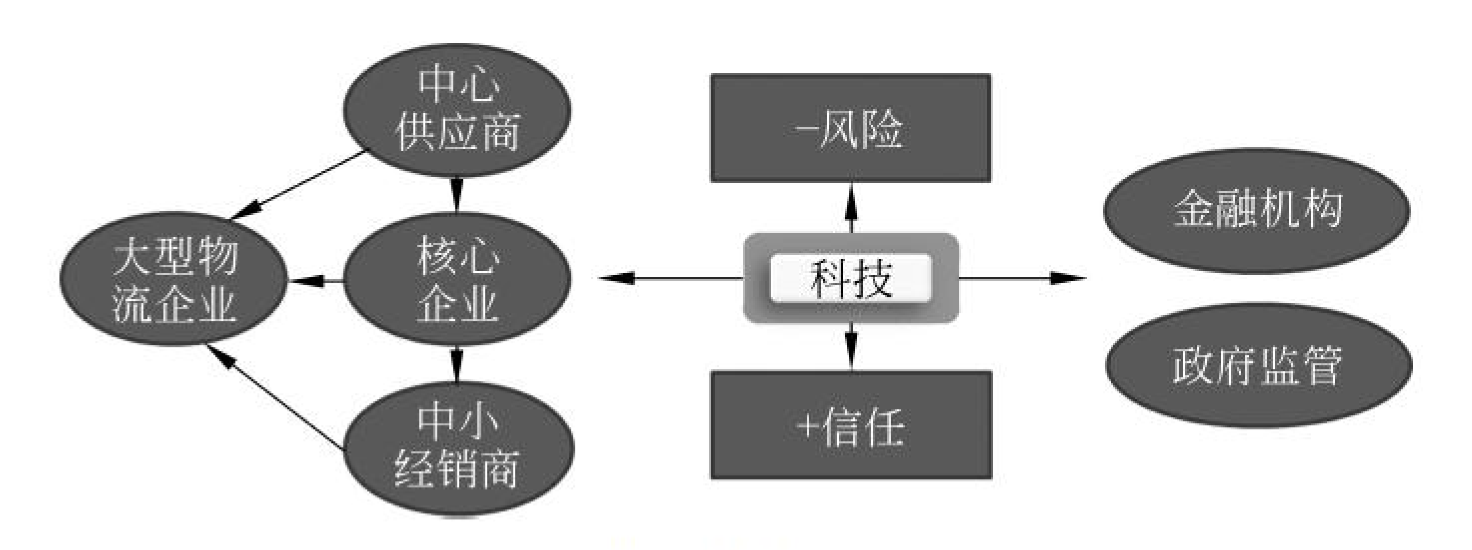


图 7.4 供应链金融核心问题

总结来看,供应链金融的核心问题有三点:融资难、风控难、监管难。

7.2.3 基于区块链的解决方案

供应链金融场景中的关键需求是——如何存证供应链的关键信息;如何确保可信资质的评估;如何保障交易各方的权益;供应链的上下游核心企业和供应商之间如何建立互信,降低融资的成本。区块链技术提供的特性和这些需求吻合度很高,数据不可篡改可以让数据很容易追溯,公私钥签名保证不可抵赖,这些机制可以让上下游企业建立互信,区块链中的智能合约,可以保障各方约定的合同可以自动执行。基于区块链可信机制的供应链金融解决了供应商单方面数据可信度低、核验成本高的问题,打通企业信贷信息壁垒,解决融资难题,提升供应链金融效率,通过供应链中各方协商好的智能合约,可以让业务流程自动执行,资金的流转更加透明,极大地提供公平性。华为云 BCS 服务利用自身在供应链和区块链方面的业务和技术积累,携手合作伙伴,积极支持其供应链金融结合区块链技术的创新,服务平台提供新型的智能合约引擎支持复杂的智能合约和高效的查询,提供创新共识算法支持峰值可达 10K TPS 的高性能并发交易,为该行业的进一步发展提供了良好支撑。

如图 7.5 所示,通过多级链结合起来,在每一级区块链中实现当前范围的可信数据共享,并基于授权,按需把数据推送到下一级区块链系统中。基于共享账本以及智能合约,不但解

决数据互信问题,同时提升各方交易的效率。

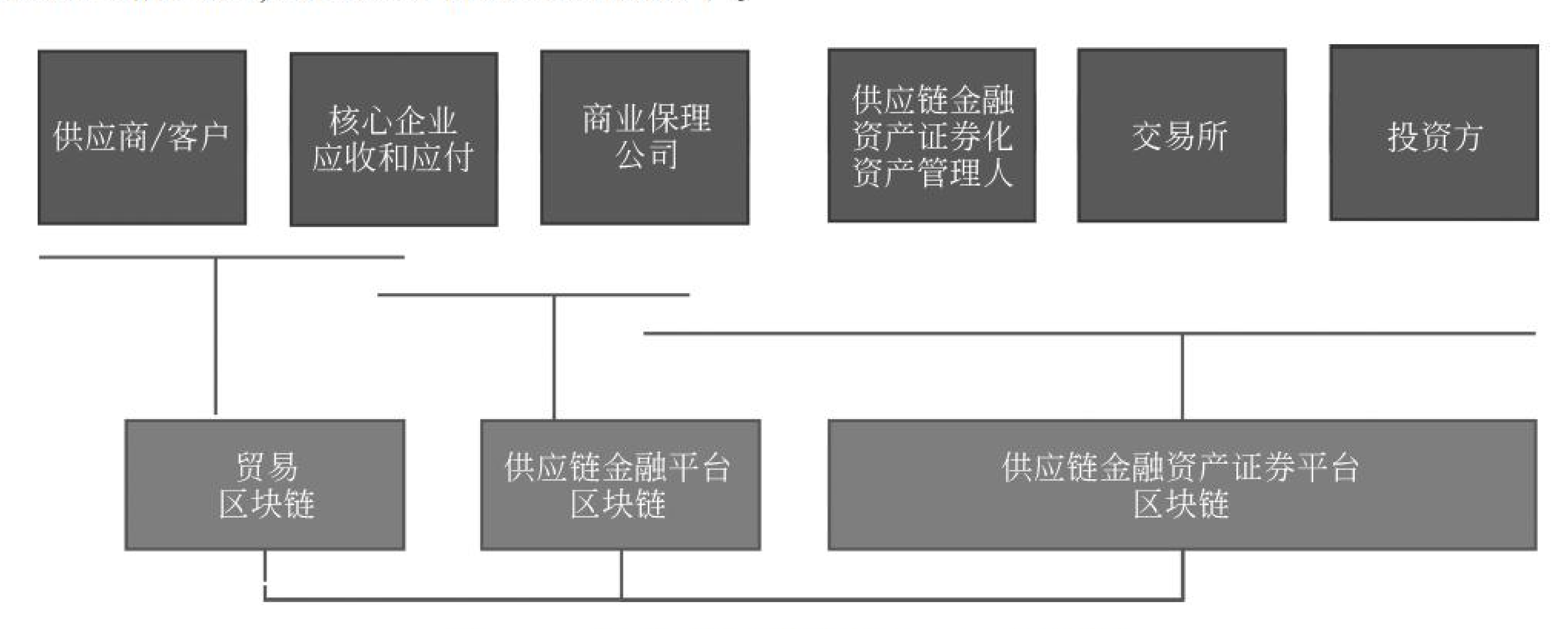


图 7.5 基于区块链的供应链金融解决方案

7.3 区块链在用户共享场景中的应用

7.3.1 业务场景

在区块链金融领域应用中另一个典型的场景是银行“认识你的客户”(Know Your Customer,KYC)系统。R3 公司曾在一份报告中提出:“传统的 KYC 流程非常复杂,而且重复度也较高。这种自我主权模式允许企业客户创建、管理自己的身份数据,包括相关资料文档等,然后他们可以授予多个参与者访问这些身份数据的权限。”

KYC 场景不仅会在金融领域碰到,现在会有众多的企业需要知道谁是他们的客户,以便能够保持安全和遵守政府的规定,例如集团公司内,各个子公司之间用户交叉共享;不同金融机构之间用户背书等,都需要涉及用户身份的确认。

这里我们通过金融机构之间用户背书的场景来介绍 KYC 的现状以及基于区块链的解决方案:基于某银行的 I 类账户以及已有的 KYC 信息背书,免 KYC 过程开通另外一个银行的 II 类账户。要求用户身份等信息需要加密,避免暴力破解,同时提供基于身份信息的快速查询。

7.3.2 行业现状和业务痛点

目前 KYC 已经成为许多金融机构、大企业商业中不可或缺的环节。当前的 KYC 流程很大程度上满足了商业与监管的要求,但是其流程越来越复杂,成本也越来越高。同时由于很多监管的需求,信息流通成为业务创建的阻碍。

现阶段 KYC 的标准流程分四个部分:

(1) 获取用户信息:根据业务要求提交客户的姓名、账户开户信息、联系方式等要素信息;

(2) 审核用户信息:机构根据联网数据进行用户数据的核实;

（3）存储用户信息：基于单点或者中心化的结构进行用户数据的存储；

（4）监控、更新、使用用户信息。

基于目前的业务流程，最大的业务痛点是数据监管与数据获取。用户数据属于隐私保护范畴，现在政府的监管法要求越来越高，各个国家、行业的标准也不尽相同。机构之间如何理解、执行 KYC 程序造成很多业务对接困难以及数据监管困难的情况。另外数字化的信息如何安全的共享获取，更是一把双刃剑，如何在即保障用户隐私的前提下，同时提供可信的数据共享，是当前迫切需要解决的问题。

7.3.3　基于区块链的解决方案

在我们的 KYC 案例中，如图 7.6 所示，A 银行将用户的身份信息通过哈希生成唯一的加密后的数据存入区块链中；B 银行不需要 A 银行共享实际的用户数据，只需要用户提供基本的信息，通过哈希计算及区块链查询两个步骤就可以进行身份确认。显著降低了金融机构的成本，同时为用户提供了良好的用户体验。

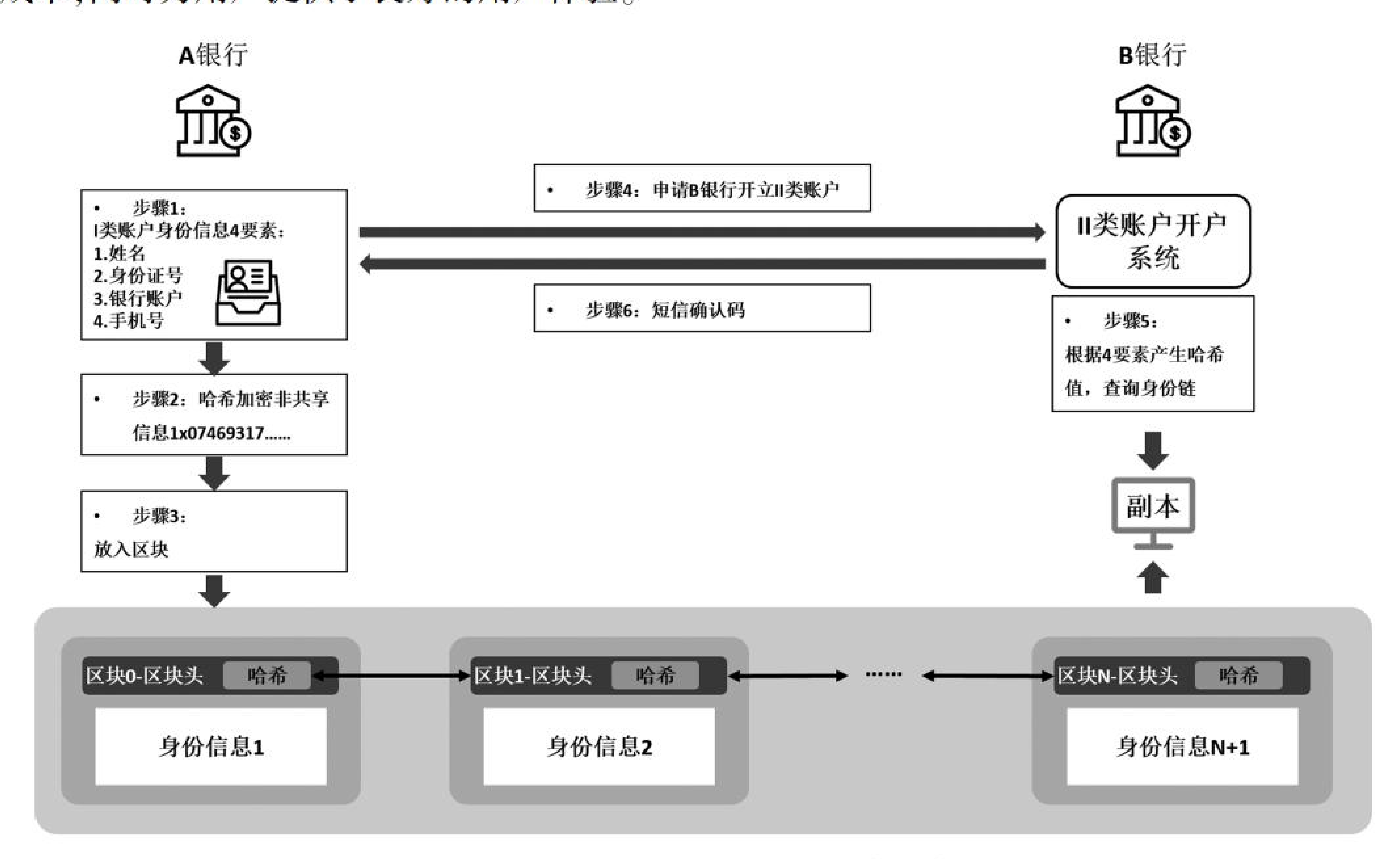


图 7.6　基于区块链的 KYC 解决方案

当使用区块链后，这些问题都迎刃而解，基于安全隐私的前提下，企业创建自己的身份数据，允许其他业务访问所需数据，而不泄露用户信息。同时企业可以提供基于身份的共享，可以快速构建企业间可信数字身份体系，这不但为企业之间业务构建打通了快速通道，同时为用户提供了一致的用户体验，增强客户黏性。

7.4 本章小结

本节主要阐述了在区块链应用最活跃的金融领域的典型案例,分析了常见的金融场景如跨境清算、中小微企业的贸易、融资和银行 KYC 的用户痛点问题和基于区块链的解决方案所带来的优势。区块链与跨境支付的结合,利用区块链去中心、分布式账本特点,实现点对点交易,打通中间环节、构建可信交易,最大限度提升效率、节省成本开支。区块链技术与供应链金融结合,保障数据不可篡改,让数据很容易追溯,公私钥签名保证不可抵赖,让上下游企业建立互信;区块链中的智能合约可以保障各方约定的合同可以自动执行,降低核验成本,打通企业信贷信息壁垒,解决融资难题,提高供应链金融效率;通过供应链中各方协商好的智能合约可以让业务流程自动执行,资金的流转更加透明,极大提供公平性。区块链技术与银行 KYC 的结合,银行企业可以创建自身客户的身份数据,且可以提供基于身份的共享,快速构建企业间可信数字身份体系而不泄漏用户的信息。

第 8 章

供应链应用案例

8.1　业务场景

供应链是人类社会活动中非常复杂的一套系统工程,参与方包括商业活动中的核心企业、供应商、物流运输企业、客户等,内容包括整个流程中的信息流、物流、资金流。如图 8.1 所示,一般来说制造业的供应链从采购的原料开始会涉及生产、加工、包装、运输、销售等环节,所以供应链在主体上会涉及不同的行业和不同的企业,在地域上可能会跨越不同的城市、省份甚至是国家,供应链整个流程中的上下游本质上是一层层供应商和一层层客户的关系,每个前方的业务和发展都和后方的供应有密切的关系。

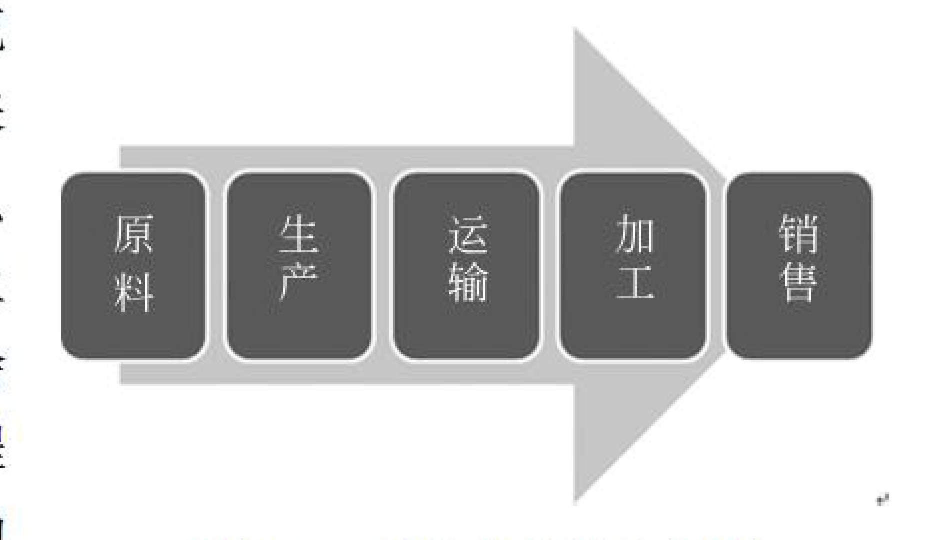


图 8.1　传统供应链流程图

从业务上看,供应链有多种,如制造供应链、食品供应链、危化品供应链等,他们的共同特点就是不同的企业相互合作,结合自身优势组合成一个规模庞大的、有竞争力的商业联盟在市场上为用户提供商品或服务。整体表面是一条供应链,同时它也是一条价值链,通过每个节点的加工、运输、包装都提高了整个商品的价值,也为每个节点带来了利润。每个环节对整个业务参与方都至关重要,每个节点的材料质量、供应效率都会直接影响整体的效率和收益。

一个案例[①]如 2000 年 3 月 17 日夜晚,飞利浦的半导体生产基地发生了一场火灾,虽然火很快被扑灭,但是已经使得大量生产线陷于瘫痪,飞利浦是多家手机厂商的供应商包括爱立信和诺基亚,这次火灾直接影响到了下游客户厂商诺基亚和爱立信的手机业务,诺基亚根据自己在供应链管理中的经验和敏锐性迅速调整,增加芯片供应商,将损失降到最少。而爱立信由于上游厂家无法及时供货,没有及时识别风险,供应链响应机制迟缓导致了后续业务上的损失。

8.2 行业现状和业务痛点

供应链的管理对于链上的企业生命都至关重要,高效的、低成本的运作是供应链管理的目标,传统的供应链管理在信息网络技术的基础上已经有很大进步,包括常用的 OA 系统、ERP 系统等都有效地支撑了供应链系统的运转,然而由于传统的技术架构的限制,各方的信息系统数据无法做到有效可信的同步,信息流的同步较为低效,其次各方系统的数据都是各方独立集中的管理,有一定风险会遭受到有意无意地篡改,对于外部不法黑客的防护也只能在系统的外部增加防火墙策略和安全设备,不能通过技术底层协议来解决这类问题。

供应链信息孤岛现象不能有效解决是影响提高整体行业效率的重要原因,比如在涉及进出口的供应链业务场景中,相关企业都需要到海关办理相关手续,这些流程往往需要专人甚至专门部门负责,从而也还带动了报关行业的发展。但是报关手续的流程复杂、业务场景面广、容易出错都会影响企业进出口的效率,这些现象的有效解决可以带动整体经济的发展,可以减少货物积压,提高通关效率,加快供应链的物流、资金流、信息流的传递。当前,政府也在积极推动无纸化的报关落地,此举也会加快该行业业务的信息化、自动化落地。

8.3 区块链如何赋能供应链及对应价值

区块链技术的出现进一步为供应链中几个痛点问题从协议层带来了很好的解决方案。如图 8.2 所示,区块链中联盟各方都持有账本数据,并且数据的增加、修改、删除等动作都必须执行各方共同制定的智能合约并共识后才能落入最后的数据账本中。由于账本数据会存储在联盟各方中,这种方式很好地保证了数据的高可靠性,任意一方数据的丢失和损坏都不会造成太多影响,它可以快速从其他方恢复数据。另外,这种技术架构也可以很好地保证任意一方都不能私自对数据进行变更,所以和各方的相关业务方面



图 8.2 供应链 + 区块链中的各联盟方

① 案例引用来源于 http://www.sohu.com/a/278589630_472865

的权利义务都可以通过智能合约来保障，有效地解决了公平、安全的问题。

我们从如下几个方面总结来看区块链给供应链行业带来的几个方面的好处：

1. 可追溯性

可追溯性是区块链的特点，也是供应链行业的需求和痛点。社会上近几年发现的丑闻也都和没有高效的可追溯机制有关，如食品方面的三聚氰胺事件、药品方面的假疫苗事件等。由于系统复杂，数据冗余和隔离，导致不能快速、有效、精准地追责和召回有问题的商品。区块链系统由于数据不可篡改，并且数据存储在联盟各方，过程中产生的数据可以实时获取，精准定位和追溯。区块链中记录的数据包括产品原料从哪里取材、中间在哪家工厂生产、商品在哪里包装和加工、由哪家企业负责运输、销售到了哪些城市和哪些超市等，这些信息在区块链系统中可以快速地获取，对于应急处理社会公共事件有很好的帮助。

2. 不可篡改性

一方面，传统的系统中数据经常会遭到黑客的攻击，入侵后数据修改对业务会造成很大的影响，企业的品牌影响力也会下降；另一方面，系统内部的管理员存在为了各种目的对数据进行获取和修改的风险，这些场景都从技术层面无法保证，需要额外的管理成本来解决此类问题，而区块链技术通过巧妙地利用数字签名、加密算法、分布式存储等技术有效的从协议层面解决了篡改的问题，极大增加篡改难度，从技术上保障了数据不可篡改性。

3. 透明性

透明性体现在多个方面，数据方面由所有链上商业方共有，所有数据对每个节点都是透明的，任何一方都可以实时获取数据进行核查和分析，比如供应链金融上的金融机构可以看到业务方的回款情况，经销商可以看到产品的质检报告等，这些特性会极大提高业务商业互信，加快链上物流和金融的流通效率；透明性的另一个方面主要体现在智能合约上，供应链上的智能合约由商业各方共同制定，内容和各方的利益息息相关，它们利用智能合约代替传统的契约和合同，让它不以其中一方或者多方的意志为转移，达到公平的效果。

这三个特点是区块链技术的优势，同时也是供应链行业的痛点问题，所以区块链技术在供应链行业应用和落地有着天时地利的条件，不少细分行业中业务全流程信息可视化、业务数据的一致认可、降低协作成本等方面有着强烈的诉求，社会也期待在这些行业中有实质性的技术创新和进步，包括食品安全、疫苗溯源、药品和器件溯源等都是全社会关注的重点问题。在食品安全领域，面临的主要挑战包括食品安全事故时责任方不愿拿出数据，物流信息可视化一对一对接导致运作成本高。区块链的分布式账本以其多方记账、不可篡改的特性恰好解决该领域的问题，实现供应链追踪，保障食品全流程安全。典型的案例如 IBM 和沃尔玛合作，对食品从种植、加工、运输、上架等全环节进行记录和追踪。IBM 在 2017 年 8 月宣布和雀巢、沃尔玛、泰森食品、联合利华等建立食品安全联盟，在更大范围探索在食品领域应用。

从业务角度讲，区块链技术可以解决供应链和溯源类场景的两大问题，一是提高业务参与方的造假成本、二是在出现商品事故后可以提高定位和召回效率。

由于联盟链的加入有准入机制,而且特殊的行业中业务参与方还会包括政府的监管单位,加上写入区块链的数据都会包含参与方的数字签名,所以一旦发现数据真实性问题,相关的企业和组织无法抵赖,假数据的操作会对其诚信和品牌造成极大恶劣影响,甚至要负法律责任,因此提高了企业的数据造假成本。溯源的区块链系统会对商品的基础属性、检验信息、物流和加工信息做详细的记录,出现事故后可以在区块链上快速找到商品的销售地域情况,对控制事故影响范围和召回工作有很大帮助。

华为公司内部有不少部门也处在供应链业务生态的一方,他们既是上游核心企业、也是下游供应商和生产商,每年有大量的人力和物力投入在供应链交付的场景中,所以公司内部也在积极探索基于区块链技术在供应链的创新。

场景一:图 8.3 是一个基于华为云区块链服务 BCS 构建的商品溯源业务场景图,该系统是一个典型的联盟链,参与方包括生产方、加工企业、运输企业、销售公司和监管单位,该系统的构建利用了 BCS 基于租户模型的联盟链构建能力,各方作为独立的云租户,对应的数据、资源和网络相互隔离、互不可见。共识机制采用了高可用的拜占庭共识算法,智能合约规定了商品的生产、加工、运输、销售整个生命周期的状态变化,通过判断各方每次交易所带的数字签名,保证商品的状态更新都需要对应的角色完成,从而维护了各联盟方对数据操作更改的权利。该解决方案通过各参与方维护商品生产周期中和自身业务相关的数据,从而完善了商品的从生产到销售的过程跟踪。后续通过定制化增加海关和港口联盟方还适用于涉及进出口的物流场景,系统能力通过增加积分模块还可以解决物流中资金流的管理和维护,进一步提高物流系统效率。

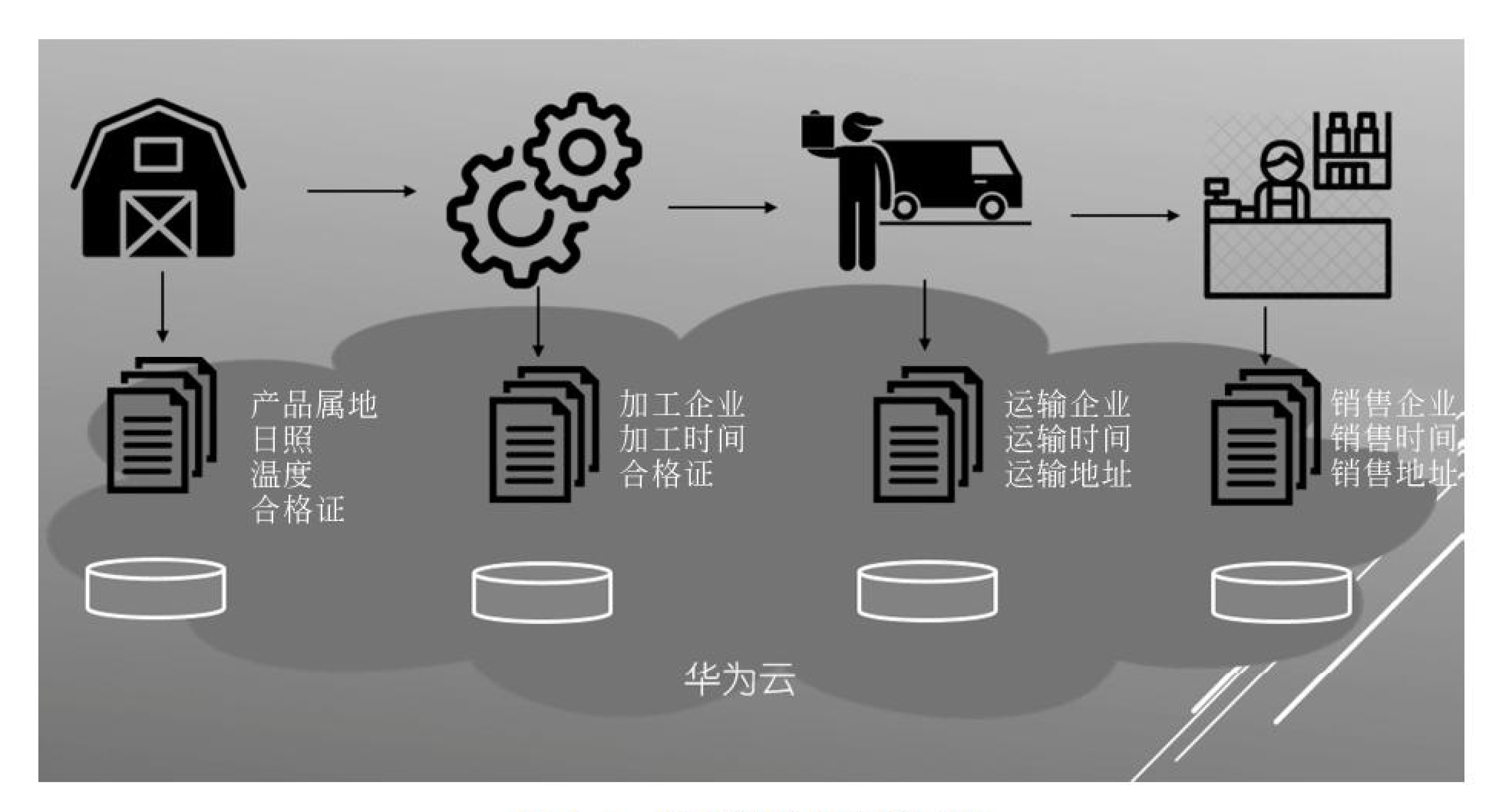


图 8.3 商品溯源业务场景图

场景二:基于华为云区块链服务的物流运输区块链解决方案,华为本身是制造大厂,有大量的设备如基站和服务器需要通过物流发送给客户,物流过程参与方众多,流程复杂(如

图 8.4 所示)，各参与方分别使用不同的信息和物流管理软件，存在以下几方面的困难和挑战：承运商签收不实时，签收单返回周期长导致结算周期长；收货地址变更管理不佳；客户签单后投诉未收到货；没有有效防丢失手段；签收单大部分为纸质单据，不便于管理；多层转包的情况下，物流过程不能做到实时化和可视化。

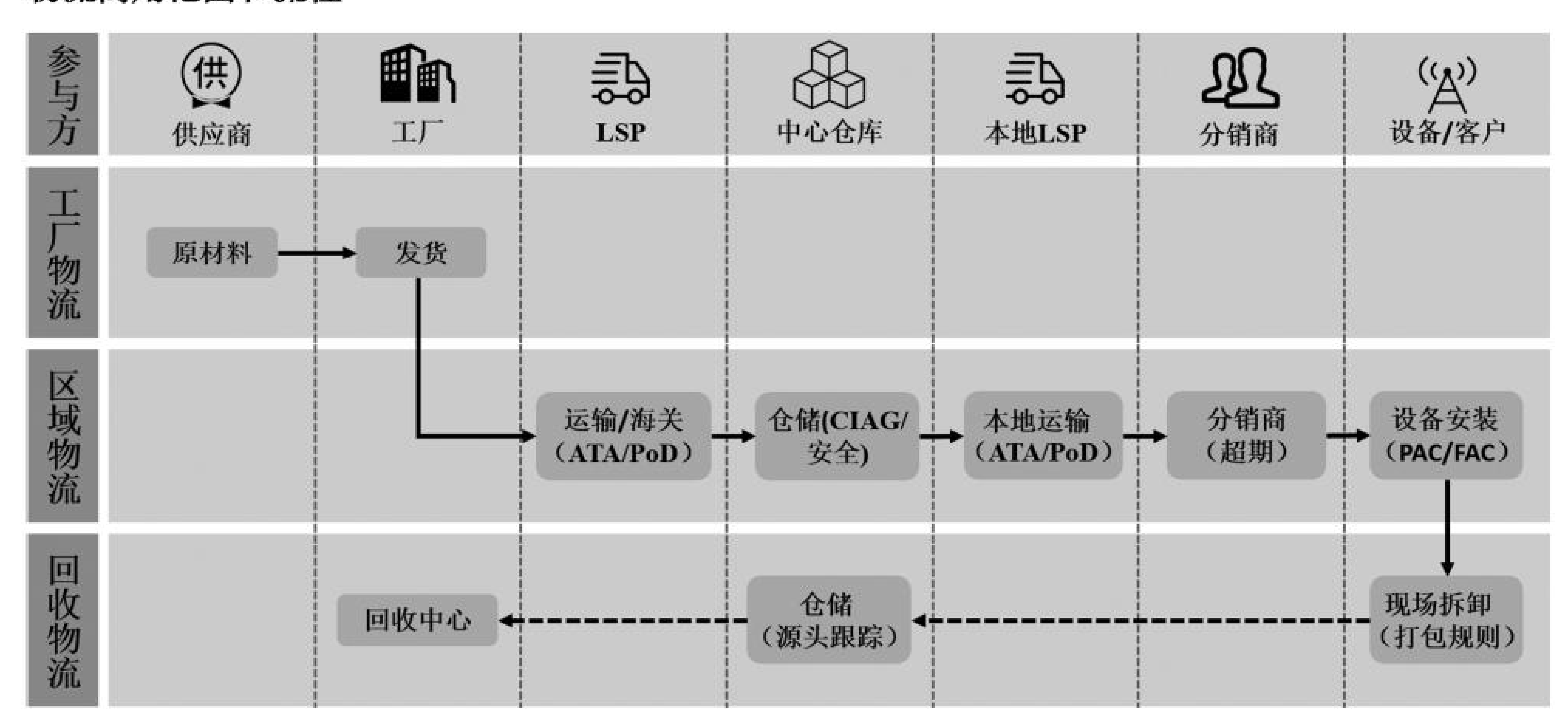


图 8.4　物流商用范围和流程图

区块链物流解决方案流程，流程如图 8.5 所示，具体流程包括：

(1) 将各业务参与方，包括制造商、物流承运商、干线运输商、末端派送商、客户，组成一个联盟，利用区块链平台，以适当的手段激励各个节点进行数据记录。业务发生时数据多方同时确认并提供不可篡改的记录。

(2) 运用区块链技术，定义各方所需要上传区块链的信息，承运单号绑定货物信息，并依

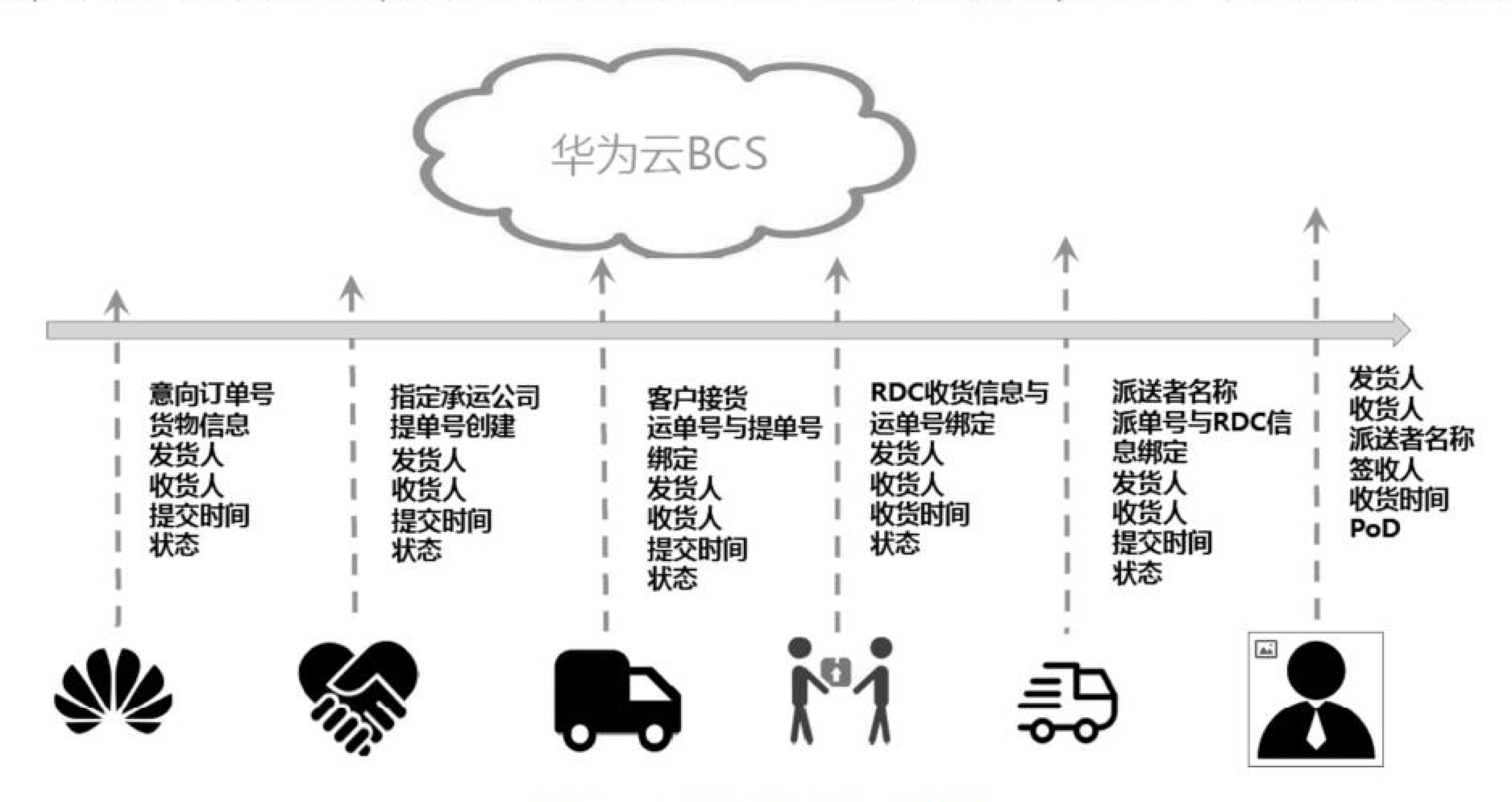


图 8.5　区块链物流流程图

次与下游或下级合作伙伴指定要通过区块链共享的信息。

(3) 分包商的单号绑定,以承运单号串起货物的整个物流过程,整体打通华为、承运商、干线运输商、区域配送中心(RDC)、末端派送等各参与方孤立的信息系统,各参与方流转信息及时上传区块链。开发供各参与方使用的应用程序(如APP或小程序),参与方分配账号,通过登录账号扫描单号转移与接收,确认货物的当前责任承担方。并通过账号授权管理,只有指定账户才能发起地址变更,从而实现客户地址变更管理。账户通过应用程序确认接收,等同于该账户所有人签字接收,账号所有人可通过账号授权他人代签。

(4) 物流过程中各方追溯信息追踪记录存储在区块链上,实现及时货到付款(PoD),区块链上信息真实有效、不可篡改,便于精确追溯与责任界定,防止货物无故丢失。

(5) 调用后台管理系统,Web端可视化展示物流过程,实现全面电子化管理,纸质单据作为参考。

(6) 实现物流过程中承运商、干线运输商、末端派送各级分包商等各参与方的客户身份识别及管理,可对其进行相应的评级与打分。

(7) 区块链加密算法和授权访问机制,让数据安全性和隐私性俱佳。

场景三:华为云BCS和SAP BaaS合作,开发展览设备临时海关进出口(ATA Carnet)区块链管理创新项,如图8.6所示。展览设备临时海关进出口是世界海关组织为暂准进口货物而专门创设的。中国海关通常免税复进口期限为6个月,要求货物原状原样原箱复进口,与出口时完全一致。每年需要到全球各大展区进行设备展览,需要将设备从国内发送到各国展区,物流和运输涉及众多参与方,同时需要进行临时海关报关和合规性检查,目前物流信息系统为各方独立拥有,无法有效全程跟踪和管理,迫切需要提高和改善整个物流和海关合规申报流程。

临时展品进出口流程涉及多国海关,华为云BCS和SAP BaaS计划合作基于双方区块链平台开发构建可信共享、全程可追踪的区块链跨洋物流管理创新项目,如图8.6所示,将ATA单据、物流过程、处理流程、货物状态都记录到带时间戳不可篡改的共享账本中,各参与方尤

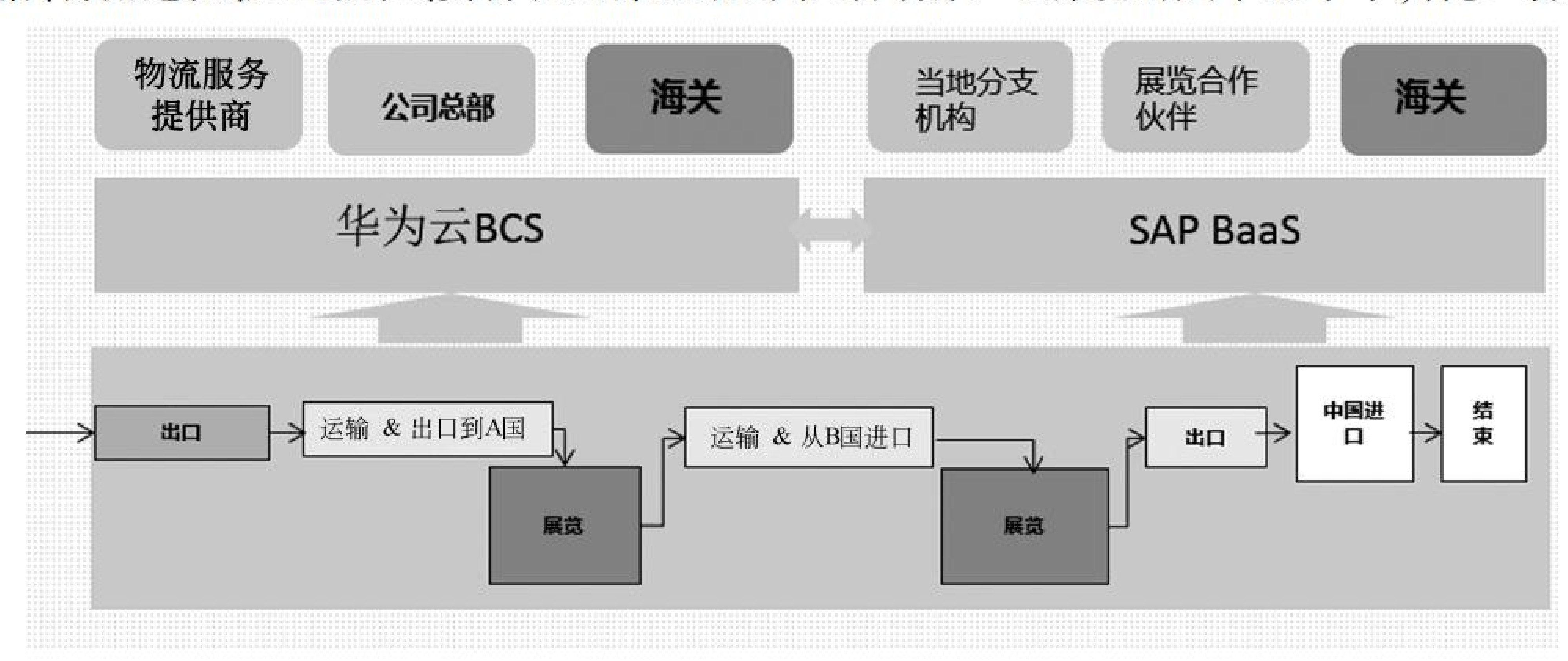


图8.6 区块链跨国物流流程图

其是海关可直接检查和跟踪临时展品进出口实时状况,这将极大改善跨国物流和海关合规申报流程,对整个流程实时追踪,提高效率。

8.4　区块链结合供应链面临的机遇和挑战

挑战一:业务数据是否真实无法单独通过区块链技术来保证,基于区块链技术的溯源场景是供应链的一个细分行业,包括食品溯源、药物溯源、器件溯源等场景,它们共同的诉求都是希望业务过程中产生的数据对各方透明、容易被追溯、数据真实可信、产品安全可靠。然而业务数据是否真实无法单独通过区块链技术来解决,参与方写入数据是否和现实数据一致目前主要由管理手段来规范,迫切需要结合物联网技术保证数据来源的可靠性。

挑战二:供应链的区块链系统需核心企业的上下游多方共同参与,任意一方的缺失都会导致整个商品生命周期信息的缺失,这也是当前该行业的重大挑战。供应链系统能否顺利组建及长久运营关键在于业务各方对该模式的认可程度。

面临的两大挑战需要社会先驱者不断探索实践、总结经验教训、摸索新的解决方案,目前区块链系统可以增加联盟各方的造假成本,提高业务流整体效率,在一定程度上推进了区块链的普惠进程,区块链技术在赋能供应链的业务转型过程中将会在该行业掀起一波创新巨浪,协议层使用区块链技术保证数据的可靠、可信,同时加快信息流动和数据共享,提高业务效率。业务层结合供应链场景、金融场景解决商品数据的溯源、物流信息的追踪和上下游企业的融资问题,跨境场景还可以利用数据共享能力提高通关效率、降级货物积压时间,支付场景可以利用区块链来完成商业企业间的自动支付和跨境支付等工作,提供资金的流动效率,降低资金清算成本。

据有关机构预测,中国到 2020 年供应链的市场规模将达到 3 万亿美元,所以供应链行业对整个城市和国家的经济发展举足轻重,各行业巨头企业包括华为、IBM、沃尔玛等公司都在积极探索和验证利用区块链技术解决自己在供应链行业的难题,相信经过几年的探索实践,区块链技术一定会大规模应用在供应链领域,创造出新的商业运作模式,进一步提高人类的协作效率。

随着区块链的供应链系统的逐步发展和完善,该行业会迎来重大机遇,后续根据链上企业的业务行为表现,还可以构建企业诚信档案,为完善社会企业诚信建设提供数据和技术支撑,税务、证券、工商等机构也会希望加入这个可信的大生态系统中,既可多维度完善社会企业可信数据,又可以从其中获取可靠的数据来支持自身工作的高效开展。如证券公司可以通过授权从企业的供应链系统区块链上获取其交易数据,为广大投资者提供有效可靠的数据。基于此类科技和业务的有效结合和发展,人类社会将会更加智能、更加可信。

8.5 本章小结

供应链和物流参与方众多、没有强中心化组织、流程复杂，这些特点在传统的中心化结构中存在过程不透明、难以追踪、管理困难等问题，而区块链的多方共享、不可篡改账本，多方共识，全程可追踪等特点刚好适合供应链和物流行业。业内普遍认为供应链和物流是最适合区块链落地的场景之一。本节系统性地介绍了供应链和物流场景、行业发展的现状和面临的痛点。通过基于华为云的几个供应链和物流行业的应用创新项目，为读者阐述了在实际应用场景中如何通过区块链解决供应链和物流面临的调整和困难，达到优化流程、提高效率、降低成本的效果。

第9章
政务服务应用案例

党的十九大报告中明确指出了未来政务系统的发展方向是由互联网、大数据等网络构成的网络综合治理体系,而区块链技术的分布式、透明性、可追溯性和公开性与政务“互联网+”的理念相吻合,它在政务上的应用也会进一步推动政务“互联网+”的建设,并对政府部门和广大群众带来非常大的影响。2017年5月26日,国务院总理李克强向中国国际大数据产业博览会发去了贺信,并首次提及区块链。李克强总理在贺信中表示:“当前新一轮科技和产业革命席卷全球,大数据、云计算、物联网、人工智能、区块链等新技术不断涌现,数字经济正深刻地改变人类的生产和生活方式,作为经济增长新动能的作用日益凸显。”区块链技术作为下一代全球信用认证和价值互联网基础协议之一,越来越受到政府的重视。本章节主要通过房屋租赁案例、税务案例及财政票据案例阐述区块链技术如何应用于政务服务。

9.1 区块链在房屋租赁场景中的应用

9.1.1 业务场景

2016年2月29日,国务院总理李克强主持召开国务院专题会议,提出对北京城市副中心和集中承载地的具体要求。3月24日,习近平主持召开中共中央政治局常委会会议,同意定名为“雄安新区”。2017年4月1日,中共中央、国务院印发通知,决定设立河北雄安新区。通知中将此新区定位为“千年大计、国家大事”,“是继深圳经济特区和上海浦东新区之后又一具

有全国意义的新区”。新区主要任务是成为“北京非首都功能疏解集中承载地”。

2017 年 12 月 6 日,李克强总理在国务院常务会议中指出:“打通数据查询互认通道,逐步满足政务服务部门对自然人和企业身份核验、纳税证明、不动产登记、学位学历证明等 500 项数据查询等需求,促进业务协同办理,提高政务服务效能,避免企业和群众办事多头奔波。”国家政务系统应号召在多个业务系统中启动基于区块链的政务解决方案如雄安将构建基区块链的住房租赁平台、基于区块链的拆迁平台等。

传统的房屋租赁的业务主要是通过下面几步才能完成一个房子的出租。首先是找房阶段:租客一般在租房信息网上查找房源或者通过电话联系中介,确认好房屋的位置和时间,然后去看房,在经过多次看房后选择出自己可以接受的价格位置,付定金、签合同、准备入住。第二是入住期间:选择中介租房的,一旦签订合同,租客和房东都要支付中介费;相当数量的租赁房需要租客自己购置家具、家电设备。第三是退房环节:由于租房期间的自然损耗,押金往往无法全额退还;租客自己购置的家具家电设备处理是难题,无论是搬家还是贱卖都是麻烦。另外,租客最大的困扰是,即使签订租房合约,也会面临房东随时解约或涨房租的风险。

雄安房屋租赁则是由政府主导的新模式,因为过度依赖土地财政推动城镇化建设的发展模式,一定程度上抑制了居民消费和市场主体活力,出现资源配置失衡、投机炒作、房地产价格上涨,易产生经济运行和金融风险等问题。中央给雄安的定位有一点,就是改革开放的先行区,也包括对房地产管理的改革。能不能通过雄安找出一个既能够发展房地产,又能够控制房地产价格,还能保证更多需要有住房的人有房住的解决方案,是区块链场景需要解决的重要问题。

9.1.2 行业现状和业务痛点

近年来,国家推出多项举措,大力推进住房租赁市场发展,以促进我国住房市场“租购并举”。住房租赁市场广阔,从去年开始,多家互联网机构和不少知名房地产企业进入住房租赁市场。

目前,主要存在于租房场景中的一个核心问题就是如何确定“真人、真房、真住”。譬如,通常租房第一步大都是找中介,而有不少人在找中介时,遇到了不少黑中介,被欺骗了时间和金钱。租房找到了好房源,往往需要商谈租房的费用,这其中就涉及中介费和押金的问题。租房人群中有相当一部分就是刚毕业的大学生,对押一付三的押金,他们有很大的压力,所以他们会寻找无押金或押一付一的房子,所以也会中一些黑中介的陷阱。房子住进去之后也不可以放轻松,房屋维修的后续服务是需要关注的。某些租赁公司出租后的服务态度不友好,在日常的房屋维修上,也不会给予相应的帮助,只有租客自己动手解决。同时,房地产交易市场在交易期间和交易后的流程中,还存在缺乏透明度、手续烦琐、欺诈风险、公共记录出错等问题,这就大大影响了租赁市场的健康发展。

对于政府等监管部门来讲,传统的中介式租房模式也有很大的弊端。合租房的非法改建,电线、电器设备不达标,存在消防安全隐患,曾出现过的出租屋火灾事件就是导致这种问

题的一个典型例子。由于个人出租房屋的极度分散性,政府无法监管流动人口,成为对毒犯、逃犯等高危人群的监管漏洞。房租一般都是私人转账完成,没有财务账目体系,没法有效征税,造成税收损失。

9.1.3　区块链解决方案对房屋租赁的价值

雄安新区管委会曾发布雄安新区购房政策的相关信息,明确提出要将房产等相关信息存储在区块链平台中。雄安新区管委会在阐述“数字雄安”的框架时,也提到了三个重要领域:公民个人数据账户系统、雄安房屋租赁大数据管理系统和数字诚信应用平台。2018年2月10日,河北雄安新区管委会召开研讨会,以住房租赁积分为切入点,探讨住房租赁管理新模式。北青报记者获悉,雄安新区探索的住房租赁积分制度,将从住房租赁市场主体属性、政策激励、租赁行为三方面,运用区块链、大数据等前沿技术,建立科学、有效的住房租赁积分全生命周期管理机制,营造活力、健康、有序、可持续的住房租赁生态。

在租房领域,虚假房源泛滥、黑中介横行、租客和房东之间缺乏信任、行业交易效率低下等问题一直存在。区块链的核心优势之一就是信息透明、不可篡改性,通过区块链记录的各种信息会完整、安全地存储在数据区块中,这样实现了数据的公平与客观。区块链技术的应用可实现对土地所有权、房契、留置权等信息的记录和追踪,并确保相关文件的准确性和可核查性。此外,可借助区块链技术实现无纸化和实时交易。从具体的操作上看,区块链技术在房屋产权保护上的应用,可以减少产权搜索时间,实现产权信息共享,避免房产交易过程中的欺诈行为,提高房地产行业的运行效率。

基于区块链的雄安住房租赁平台会同教育局、财政局、房管局、社保局和房屋运营企业构建起一条联盟链,在雄安一些中介也作为房屋运营企业参与其中。按理说,区块链技术的应用首先应消除的就是中介,但从中介的积极参与中,我们似乎看到了中介在去中介化过程中的另一种可能,即“从中介变为信息服务商”,成为提供房源租赁信息服务的角色。除了房东的个人信用、之前的出租记录、房客评价等信息会被上传到链上,租房人的个人信用、租房记录、房东评价也会记录在链上。同时,租售同权即租赁存证、租赁合同、转账信息等信息也会上链,如图9.1所示,租赁过程、结果透明公开实现公平租赁;使用分布式账本来保证信息共享互通达。租房各个环节信息都记在区块链上,它们之间的每个流程都会进行相互验证,租客就不必再担心遇到假房东,租到假房子,最终实现李克强总理提出的“让群众少跑腿、少烦心、多顺心”,让群众办事“只跑一次”。

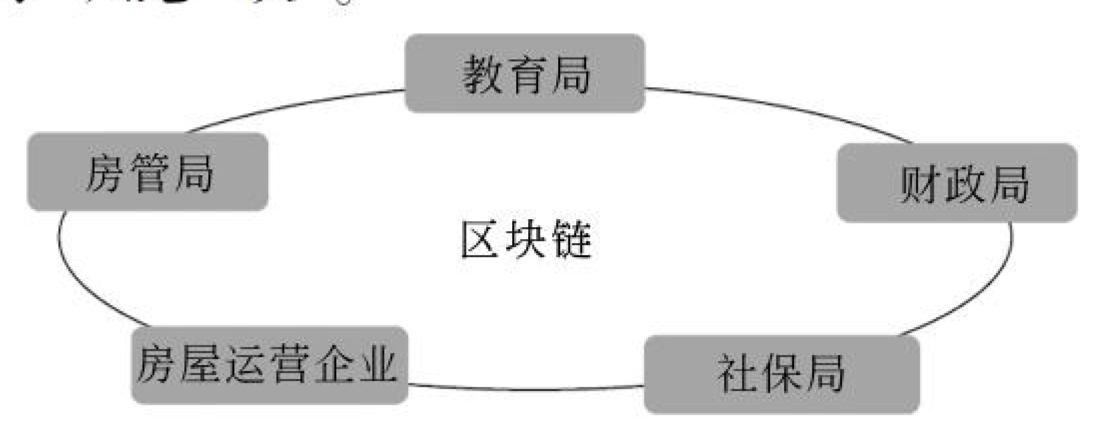


图9.1　区块链与政务系统的结合

9.2 区块链在税务变革场景中的应用

9.2.1 业务场景

政务系统的另一个典型是：它与每个人息息相关，个人贷款、纳税都离不开它。传统的办理流程如下：有贷款需求的纳税人登录银监局平台申请办理贷款，需要提供纳税信息时，跳转到税务网厅指定页面，查询到相关纳税信息（税务与银监局事先确认的交互内容），确认发送指定商业银行，网厅平台请求税务外部数据交换平台将相关信息发给银监局平台，银监局平台发给相关商业银行，完成上面流程才能确认此人是否有资格进行贷款。而企业贷款是根据一段时间内的税务信用等级、销售收入、利润、增值税、企业所得税等关键指标所反映的企业的信用状况和盈利能力，适用于作为银行评估中小微企业贷款能力的一个指标与凭证。为了确保个人及企业纳税凭证的真实有效，税银贷款业务通常以纸质材料形式办理。在票据方面，是通过“以票控税”，我们主要依靠发票来证明业务的真实发生。而缴纳个人所得税，开完税证明需要跑到税务局现场才能办理。

如果基于区块链的税务示范系统优化上述场景的问题将带动区块链在政务应用的爆发性增长。

9.2.2 行业现状和业务痛点

近年来，税票在各领域作用日益凸显，纳税人办理各项事务时，经常需要提供完税证明。过去，这些税票必须到办税服务厅申请开具，办理时间、地点受到很大限制。纳税人来到办税大厅、排队、叫号，再打印税票，遇到人多的时候，从开始到拿到完税证明，再去申请个税补贴，往往需要花上很长一段时间。

另一个痛点就是贷款方面，小微企业用款讲究的是“短、小、频、急”，传统银行信贷业务的风控体系主要是基于线下的尽调和审查，以客户的身份信息、资产信息、资金流信息为主要的数据源，覆盖用户有限且效率低。银行要打破原有的传统审批方式贷款才能真正服务小微企业融资，足够刚性的数据成了痛点。

税务系统以票控税，对消费者而言，传统发票在完成交易后，需等待商家开票并填写报销单，经过报销流程才能拿到报销款；对商户而言，传统发票在消费者结账后需安排专人开票，开票慢、开错票等问题很容易影响消费体验。有些人还会大量虚开发票，甚至是“暴力虚开”，为税务管理和行政监管带来了极大的挑战。

9.2.3 区块链解决方案对税务系统的价值

国家倡导“让数据多跑路、群众少跑腿”，税务部门也在通过区块链技术践行国家倡导。腾讯联合深圳国税及金蝶软件，打造了“微信支付——发票开具——报销报账”的全流程发票

管理应用场景；华为目前跟某税务部门联合实现了基于区块链的税票管理系统的原形验证，采用区块链系统后整体方案如图 9.2 所示，将总局、各省市税务局、各地方银行构建起联盟链，将地方税务数据实时上链，保证总局可以查看地方税局的数据，各个地方税局无法互相查看，地方税局和地方银行之间也建立通道，保证银行可以从税局取到相应的用户数据。为了满足大量用户贷款、签证、报税等大并发量业务访问，华为 BCS 服务提供创新的共识算法，峰值可达 10KTPS；为了保护个税隐私信息可验证但不泄露，BCS 服务提供同态加密和零知识证明机制，实现保护隐私的能力。

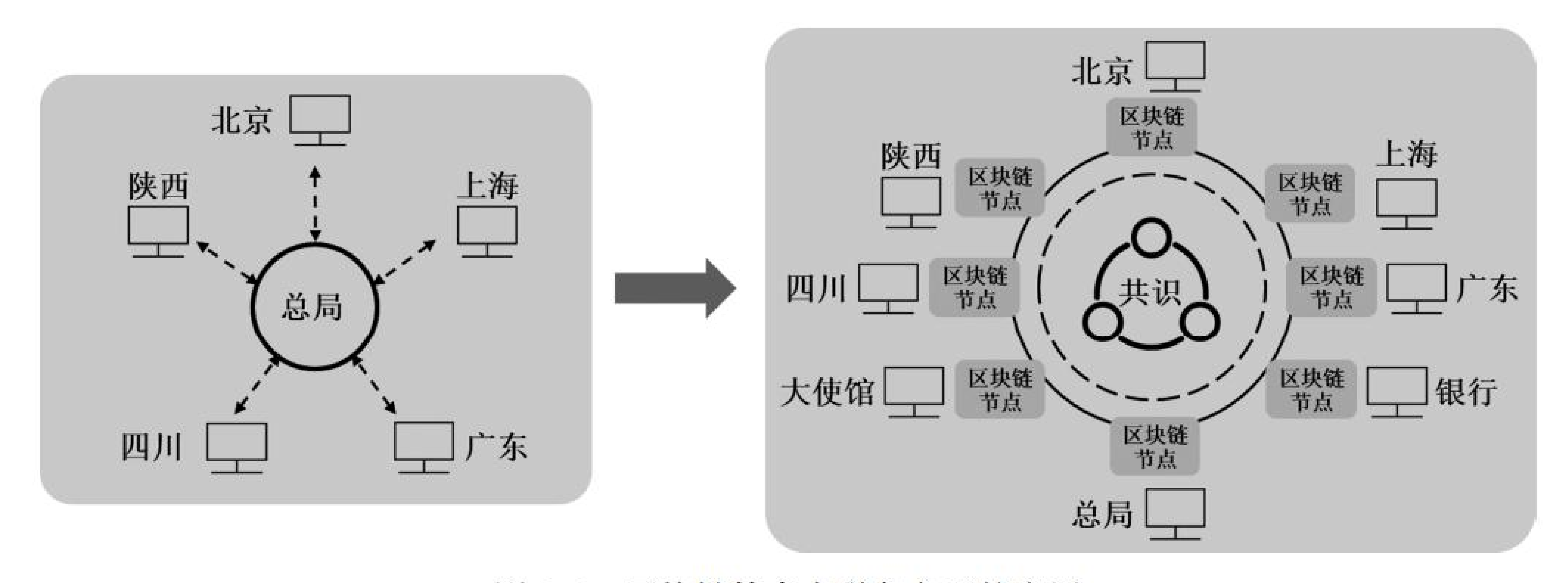


图 9.2　区块链技术在税务方面的应用

为解决小微企业贷款审批问题，将区块链技术应用于在线税银贷业务，由贷款企业授权银行查询纳税数据后，银行根据内部风控模型给予企业授信额度，以此快速实现税、银、企三方数据对接。采用区块链技术，不仅能够实现电子纳税凭证的鉴真，而且智能合约可保证数据使用授权执行、控制操作权限，并存证全流程应对争议。

区块链技术在开电子发票可以有两个重要作用：一方面，确保从领票、开票到流转、入账、报销的全环节流转状态完整可追溯；另一方面，税务部门、开票方、流转方和报销方四方可以共同参与记账，发票信息难以篡改。如果采用区块链发票后，消费者结账后可以直接从网上申请开票、存储、报销，且报销状态实时可查，实现“交易即开票，开票即报销”，基于区块链分布式账本的原理，纳税人的交易信息将真实有效，且不可篡改，进而确保纳税人的每一笔业务将不再需要发票来证明真实性；商户方则可以利用区块链电子发票极大节省开票成本，提高店面效率以及开票体验。同时，通过区块链技术架构可以建立新型数字票据业务模式，借助分布式高容错性和非对称加密算法，可实现票据价值的去中心化传递，降低对传统业务模式中票据交易中心的依赖程度，降低系统中心化带来的运营和操作风险。区块链技术还能完善监管流程，以有效规避假发票，解决发票流转过程中一票多报，虚假报账，真假难验等难题。区块链技术不可篡改的时间戳和全网公开的特性，还能有效防范“一票多卖”“打款背书不同步”等问题。

此外，银行能够掌握纳税人的信息十分丰富，如果能够将纳税人在银行的涉税资金流（包括资金的转入和转出）信息都反馈到税务局，那么税务部门就能获取到更加全面的涉税信息，提高税务部门的征税效率，有效打击偷税漏税行为。因此，在银行与税务部门之间建立能实

现可控数据共享的联盟链平台是很有意义的。

9.3 区块链在财政票据场景中的应用

9.3.1 业务场景

2017 年,财政部印发《关于稳步推进财政电子票据管理改革的试点方案》,以期全面提高财政票据使用便捷度,提升财政票据监管水平和效率,重点包括网上报名考试、交通罚没、教育收费、医疗收费等业务。该项工作此前已经在北京、厦门、广西等多地展开试点工作。对于此次的全面推开,业内人士认为,这进一步夯实了政府非税收入管理基础,让人民群众能够更加便捷地享受政府公共服务。同时实现财政管理创新,依托财政电子票据管理系统收集到的标准化数据信息,建设财政电子票据大数据应用平台,对财政电子票据数据进行挖掘分析,提供查询、统计、预测、决策等各项数据分析服务,为相关财政管理和监督提供决策依据。

9.3.2 行业现状和业务痛点

传统纸质财政票据的印制成本高、开具效率低下、管理不规范、不便于监督检查等问题日益突出,越来越不适应现代信息网络技术的发展,制约了网络缴款、电子支付等新兴缴款模式在政府性收费中的应用。为解决上述问题而开展的财政票据电子化管理改革,运用计算机和信息网络技术开具、存储、传输和接收数字电文形式的凭证,正是借助信息技术推动财政管理创新的一次有益尝试。

同时财政票据在社会主义市场经济中有着重要的源头控制作用,它是行政事业单位财务管理和会计核算的重要凭证,是规范政府非税收入管理的最基础环节,更是有效预防腐败的重要举措和检验政府部门是否依法行政的重要依据。一般而言,财政票据电子化管理借助先进的管理技术和手段,可以达到“印、发、审、验、核、销、查”全方位动态监督管理,对于贯彻落实财政工作科学化精细化管理要求,从源头上预防和治理“三乱”现象,促进非税收入收缴改革,完善财政票据管理内部控制等,有着重要的现实意义。

在财政票据电子化过程中需要解决的一个重要问题即是如何保证电子票据安全,需要构建财政电子票据安全保障体系,确保财政电子票据在生成、传输、储存等过程中,始终保持真实、完整、唯一、未被更改。区块链技术在解决这个问题上有着非常高的契合度。

9.3.3 区块链解决方案对财政票据的价值

以医院开具的财政票据场景为例,财政局、医院、社保局、保险公司、审计部门等可以组建如图 9.3 所示的区块链联盟链。

个人在医院进行诊疗并缴费后,本次诊疗的缴费记录由医院录入到区块链中并由财政局开出电子票据,同时此次诊疗缴费的信息同步到区块链上其他参与方的账本中。在这个过程

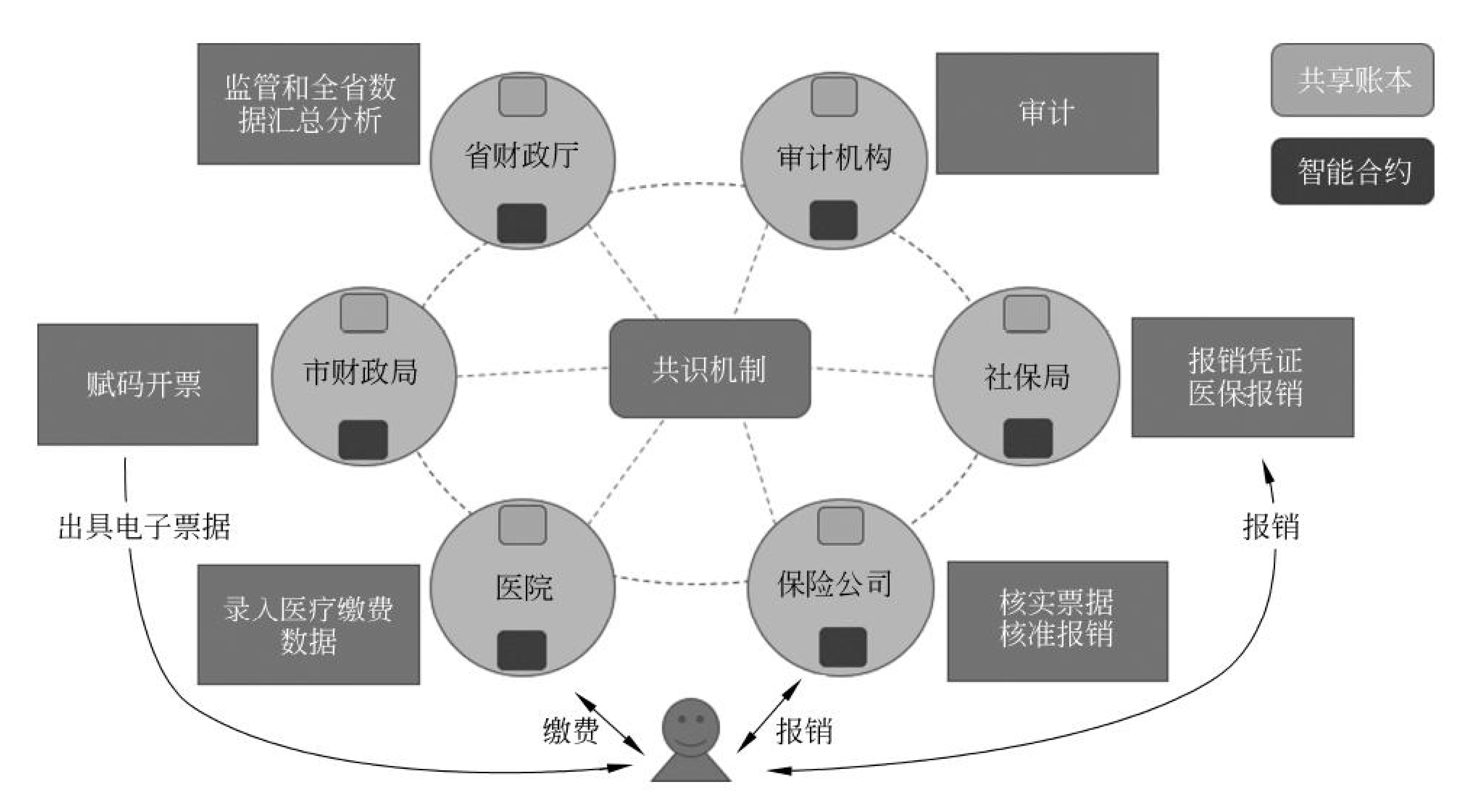


图 9.3　医院电子票据联盟链

中,区块链的技术特点将有助于在效率和安全性方面带来如下价值:

- 共享账本端到端打通了多个组织间的异构系统,使得票据数据在联盟成员间完全透明化。从而各成员可以应用该数据实现不同的功能和服务,如保险公司和社保局用于报销核实,上级财政部门用于监管下级部门及获得准确的一手数据用于分析,审计部门获得可信的数据进行审计等。并且在有权限的一方对数据进行更改后,其他成员也能实时获得更改后的信息。比如一家保险公司对票据进行核销后,其他保险公司均可获知此状态,票据将不能用于重复报销。
- 智能合约和共识机制保证了链上数据的更改权限掌握在必要的角色手中,避免了集中化的数据存储介质中,管理员权限过大可以任意篡改数据的情况。比如开票要求必须至少得到财政局的背书,防止假票据的产生。
- 多中心化和块链结构账本保证了票据数据难以被篡改,以及天然的容灾备份,很大程度上防止了由于黑客攻击等造成的安全威胁。并且由于票据的历史记录全部可以被回溯,使得审计工作的调阅成本大大降低,变得更加高效、透明、可信。而审计的工作越简单高效,就使得审计越具有威慑力,形成良性循环。

综上所述,区块链技术不仅能够为票据电子化填补上安全性这最核心的一环,并且能给上下游部门带来更大程度的效率提升,使电子票据如虎添翼。

9.4　区块链结合政务服务的机遇和挑战

区块链技术在国内外的政务系统中都有一些典型的应用。在澳大利亚,其邮政部门已准备选举投票也使用区块链来记录,防篡改、可追溯和安全性将会成为使用区块链系统的优势,

这一系统将从公司选举和社区选举逐步推广应用到议会选举中。在英国,福利基金的分配以及使用情况将被政府使用区块链技术来跟踪,并且会逐步在税收监管、护照发行、土地登记和食品供应链安全等相关方面推进。在瑞典,政府计划使用区块链技术实现土地注册系统。区块链会记录所有土地交易,土地交易会被所有相关方面实施监控,确保交易安全、没有诈骗行为。这一系统还允许所有交易相关方面监控交易进展,包括不动产中介机构、卖家、买家、相关银行以及政府土地管理部门。

在国内,早在多年前就主张推行电子病历,但由于患者隐私信息易泄露和电子病历易被篡改两大安全顾虑而阻力重重。医患争议发生时,电子病历也难以被法庭采纳为关键证据。基于区块链技术的卫生部门电子病历存证,电子签名是将医疗责任落实到人的证据指向,而区块链存证提供了不可篡改的电子证据验真记录。只有充分保障数据流通的可信和安全,才能实现电子病历的方便流转。区块链技术可以应用于政务服务中如此多的场景,并且可能还有更多的场景没有被发现,政府部门也积极在一些可能应用区块链技术的业务中进行试点,政策上也持鼓励和支持的态度。

区块链技术应用在政务领域会带来如下的三大优势:

优势一:进一步实现“互联网 + 政务服务”的优化升级。“互联网 + 政务服务 ”已经成为政府部门政务工作数字化建设和发展的趋势。信息技术已经开始广泛应用于政府机构,支撑其进行数字化管理和网络化管理,把日常办公、收集与发布信息、公共事务管理等工作转变为政府办公自动化、政府实时信息发布、公民网上查询政府信息、电子化民意调查和社会经济统计等方式。随着区块链技术的发展,“区块链 + 政务服务”的电子政务服务模式开始逐步加以使用,“区块链 + 政务服务”服务模式可以通过区块链技术结合大数据作为切入点,去解决开放共享数据所带来的信息安全问题,消除社会大众对隐私泄露的担忧,在改进政府管理能力的同时,保障公民的个人隐私不被盗用、公民自身的合法权益受到保护,每个人对自己的信息所有权都能掌握,能够实现在发展的同时保证安全。区块链技术自身具备的不可篡改、非对称加密能力、数据可追溯等特性,使得通过区块链传输的行政业务需求的数据信息具有高度的安全性和可靠性,并且能够基于共识算法构建一个纯粹的、跨界的“利益无关”信任网络的验证机制,打造一条牢不可破的网络“信任链”,确保系统对任何用户都是“可信”的,为网络交易各方营造一个高度安全、深度信任的数据流通环境。

优势二:提升服务效率并降低信息系统运营成本。政府各部门在本地部署他们的区块链节点使得其分布式账本与业务系统数据保持同步。同时,只有数据的哈希值会被存储到区块链中,并不会同步完整的原始数据。每条数据的哈希值只有数十字节,可以以极小的数据带宽消耗来实现数据记录的安全同步。减少各部门的工作量使得他们的业务数据不用全量的冗余复制到中心化数据交换系统中,还能保护部门间的数据隐私,除非他们进行跨部门业务,从而降低了信息化服务中心对中心化系统的维护负担。据埃森哲 2017 年发布的报告统计,区块链的应用将为政府监管降低 30% 至 50% 的成本,并在运营上节约 50% 的成本。

优势三:进一步促进政务公开。根据国家政务公开的相关要求,政府通过大力进行信息

化建设,目前为市民提供了便利的政务公示和查询环境,但从技术上无法避免内部管理权限泄露或被擅自使用的问题,导致违规对数据记录进行更改,更改公示信息、不予执行公示政策或不经大众达成共识却擅自执行,从而使信任隐患产生。使用区块链对数据及多方哈希进行记录同步,能够留下不可篡改且发生时间明确的数据记录。基于此记录,内部审查人员能够清楚地做穿透式监管。此外,公众可以通过区块链网络中的可信节点对记录在区块链上的数据进行真实性验证。促使政务服务变得阳光、透明、可信。区块链的应用使得政府部门的职能公信力与技术公信力叠加提升,从而更好地施行阳光型、服务型政府定位。

虽然区块链技术在政务领域有如此多的优势和场景,但是不可避免地还是会有很多的挑战,和一些不好去解决的问题。以税务为例,当涉税业务体量变得非常巨大的时候,涉及的部门领域就越来越多,需要确保数以亿计纳税人的利益。去中心化的区块链系统如何保证在如此大数据量的情况下正常运作,并且顺利解决全国范围内跨大量部门的涉税数据按需共享并且相互保密,以及保证所有数据合法性、安全性受到有关部门的监管,这会是一个巨大的挑战,也是我们今后继续研究的重点和方向。

新技术的应用可能会存在一些技术及经济上的风险,有关管理部门需要去积极引导,通过产业基金等方式为积极调研和尝试区块链技术的企业提供一定的资金支持,引导和调动试点应用区块链技术的业务系统的企业积极性,并逐步促进他们成熟发展。在加强区块链基础技术研究的同时,需要深入研究区块链技术在政务领域各个方面的应用,包括政府在金融、教育、慈善、民政、审计等应用场景,通过实践完成一些典型应用项目的开发,不断加强对区块链技术及应用趋势的较深层次的探索。

9.5　本章小结

本章主要阐述了区块链应用如何服务于政务场景,通过雄安的房屋租赁案例和税务系统个税缴纳案例,分析了常见的政务系统在进行“互联网+”建设过程中会遇到的问题和基于区块链的解决方案所带来的优势。区块链应用在雄安这个比较特殊的租赁市场,利用区块链去中心、分布式账本特点,实现点对点交易,打通中间环节,构建可信交易,最大限度提升效率,节省成本开支。区块链技术还可以应用于个税信息统计、小微企业贷款、电子发票开具等领域,借助分布式高容错性和非对称加密算法,该技术不仅能够实现电子纳税凭证的鉴真,而且智能合约可保证数据使用授权执行、控制操作权限,并实现全流程的存证,从而应对各种质疑。通过上述案例希望能为政务系统带来一些整体性的思考,以期能对政务电子化带来一定的帮助。

第 10 章

存证及版权应用案例

版权保护,又称著作权保护,实质上是一种控制作品使用的机制。作为调节创作者私人权利和全社会公共利益的机制,版权保护主要通过保护经济权益来促进公益目标的实现,而且绝大多数版权纠纷也是因经济利益而起。

作为数字产业最重要的版权制度,受基础薄弱与数字技术的叠加影响,一直以来陷入发展困境,无法有效保护原创者权益,严重制约了数字产品的可持续供给。区块链因其去中心、难篡改、可追溯、开放透明等优点,有望解决版权登记这一核心技术难题,从而为版权保护开辟一条新路。

10.1　业务场景

美国出版商协会定义的数字版权保护(Digital Rights Management,DRM)是指“在数字内容交易过程中对知识产权进行保护的技术、工具和处理过程”。DRM 是采取信息安全技术手段在内的系统解决方案,在保证合法的、具有权限的用户对数字信息(如数字图像、音频、视频等)正常使用的同时,保护数字信息创作者和拥有者的版权,根据版权信息获得合法收益,并在版权受到侵害时能够鉴别数字信息的版权归属及版权信息的真伪。数字版权保护技术就是对各类数字内容的知识产权进行保护的一系列软硬件技术,用以保证数字内容在整个生命周期内的合法使用,平衡数字内容价值链中各个角色的利益和需求,促进整个数字化市场的

发展和信息的传播。具体来说，包括对数字资产各种形式的使用进行描述、识别、交易、保护、监控和跟踪等各个过程。数字版权保护技术贯穿数字内容从产生到分发、从销售到使用的整个内容流通过程，涉及整个数字内容价值链。

目前数字版权保护方式主要通过传统版权登记保护和电子数据登记备案方式，电子备案可以有两种选择：第一，在行业协会等第三方平台进行电子数据登记备案；第二，选择技术背景强并可信的第三方支撑平台存证和认证，在数字版权归属权产生纠纷时，提供初步证据，结合官方人工登记，与防侵权相互补充。

10.2　行业现状和业务痛点

在互联网数字新时代，信息传播异常简单，普通人非常容易具备零成本复制、秒级传播的能力，产品的生产与传播日益快捷，在互联网时代的数字版权具备这样几个特点：每个人都可以成为创作者和版权人；数字内容不断进化，版权市场空前繁荣，版权意识全面提升，付费消费数字内容普遍化；数字作品碎片化日趋严重，随时随地产生，收费也趋向于小额快速结算；传播途径众多：自媒体、移动网络、游戏、短视频、微博、微信、朋友圈、阅读器等。

在这种环境下，侵犯版权几乎不需要什么代价。而在维权方面，目前业界还普遍沿袭纸质作品时代通过版权登记来确认版权所有人，然后结合公权力保障作品所有人的权益，这种在印刷品时代行之有效的版权登记确认方式，到了互联网时代就显示出其弊端，比如：流程烦琐、成本非常高昂等。在我国，通常为一件作品登记到相关部门确定版权整个流程需要数百元到数万元不等的费用，版权确定周期一般为半个月甚至几个月，因此版权登记和确认的时间和经济成本都非常高；而且即使这样获得版权也不能有效地保障作品权益，当版权被侵犯时只能诉诸法律，而举证、确权、验证等环节手段匮乏，难度和时间代价也非常大；即使最终能够赢得官司，权利人维权获得的收益与其付出也不相匹配；此外，法律制度的不健全也为侵犯版权这种不正之风提供了滋生的空间。

总的来说，现有数字存证和版权维护存在以下的问题：

- 传统的版权保护效率低，无法应对海量数字作品，网络时代的数字作品具有产量高、传播快的特点，经过登记再发布早已经丧失了内容的时效性；
- 传统的版权保护成本过高，造成了大多数网络作者并不进行版权登记和保护，导致侵权频发；
- 取证维权难。在抄袭行为被发现后，原创作者无法拿出侵权证据，在作品未进行登记与保护的情况下，难以获取具有法律效力的证据；
- 维权周期长。版权相关交易流程难以跟版权存证系统整合，导致交易周期拉长，内容生产者的活跃度受限；
- 难以形成有效市场。数字作品种类繁多，缺乏标准，内容消费的收益难以公平有效地

在原创作者和相关机构间分配,无法形成有效的市场。

综上所述,侵权容易、维权难成为数字时代版权保护首先要解决的难题。在当前互联网时代,实名制还没有有效实施,侵权人基本是匿名存在且人数众多,侵权对象较难确定;付费体系和习惯没有形成、网民版权意识薄弱,使这个问题更加难以解决。长此以往,将会导致知识创新者辛苦创新获得的回报还不如不劳而获的盗版者,使创新者失去创新的动力,整个社会将出现拿来主义盛行、创新意识淡薄的现象,此消彼长,给国家和社会带来不可估量的经济损失。

10.3 区块链对数字存证和版权的价值

10.3.1 区块链对数字存证和版权的价值

在互联网环境中,原创凭证和维权依据能给原创者带来巨大的价值,便捷、安全、可信、价格低廉的版权保护方式能更好地满足作品的传播及交易需求。

区块链由分布式数据存储、点对点传输、共识机制、加密算法等技术组合扩展而来,具备不可篡改、信息透明、可追溯和可信共享等特征,区块链和行业相结合将具备两个非常有价值的特点:一是解决跨公司、跨利益集体等多个主体之间的信任问题,实现数据孤岛的连通和信息可信共享;二是商业流程自动化,在区块链可信环境中运行智能合约,解决交易双方的信任问题,提高交易的便利性。

基于区块链技术的数字版权解决方案,利用区块链的去中心化和可追溯性能更好地保护数字资产,表 10.1 从技术层面系统地总结了区块链的特征给数字版权带来的价值。

表 10.1 区块链技术对数字版权的价值

区块链特征	对数字版权突破性的价值
多中心化	分布式存储和共识能有效地去除第三方,解决因第三方带来的维权难、周期长、成本高和赔偿低的问题
开放性	通过加密技术等开放式的区块链技术能有效减少数字产品发起人对产品的掌控,减少中间商赚取差价的问题
透明性	创作者能够通过区块链技术清楚地了解数字产品的使用和授权情况,并能直接和受众进行沟通,了解其对产品的真实想法
自治性	通过智能合约实现授权和交易透明,任何人都必须尊重版权并付出一定的费用才能获得产品,减少盗版肆虐的情况
数据不可篡改	在发生版权冲突时,区块链所记录的数据和时间能够起到重要作用,避免出现版权难举证问题

总体来说,区块链数字版权系统具备以下几个方面的优点:

1. 能快速有效地保护作者的权益

互联网时代数字产品的特点使数字版权面临新的挑战——如何快速有效地保护作者的权益。在互联网时代，数据传播的高速度使数字产业中的新技术几乎不存在保密的特性。当一种新兴技术被发明出来之后，数字产业往往比传统产业快上数倍甚至数十倍的速度将这种技术在业内进行推广，产业的特点让技术更快地投入实际的应用中，而这样的过程让知识创作者丧失了很多的权益。区块链技术能够让作者的权益获得最大的保护，让其作品版权避免被他人所侵犯。

2. 去中心化版权保护，降低版权保护成本，提高维权效率

区块链技术将给数字行业的版权保护带来新的变革，在传统的知识产权保护过程中，版权保护中心机构的执行效率和保护成本不尽人意，导致知识产权存在取证难、周期长、成本高、赔偿低等问题，区块链具有的功能刚好匹配这种市场的需求，将版权保护中心机构角色由裁判变为监督，将信息存储在互联互通、多方存储和实时共享的区块链共享账本网络系统中，无法被任意篡改，极大地提升了维权的效率，降低了维权成本。

3. 打通版权信息孤岛，构筑版权互信，形成有效数字市场，促进数字行业良性发展

区块链也能很好地符合数字行业的特性。目前数字行业处于信息孤岛模式，各版权运营商各自维护一份账本，这些账本的拥有者都可以对其进行篡改或者编造，这对于数字版权原创性保护带来极大麻烦。而区块链技术可以有效地防止账本被篡改，结合合法的时间戳，能做到入链即确权，能快速地对版权的原创性进行追溯和问责。

数字产业的创新性很强，科技的依存度很高，对日常生活渗透性最直接，版权的有效保护对数字产业的发展方向具有决定性的作用。如果版权得不到保护，后果不堪设想，区块链技术能很好地保护版权，进而纠正数字产业的发展方向，并有效地保障产业创作者等人员的收益。

10.3.2　区块链数字版权原理介绍

区块链技术和数字版权的结合为整个行业带来显而易见的变化，目前国内各大公司都在尝试数字行业和区块链的结合，这些公司基本上是通过构建区块链联盟链的方式来搭建数字版权和存证系统，原理基本相同。

系统基于区块链数字版权技术建立版权联盟通过区块链、大数据和人工智能等技术来保证创作者的版权权益，由版权运营方、版权所有人、消费者代表和可信机构搭建的区块链版权联盟链，每一条版权信息任何人无法篡改且随时可追溯。公证处和版权局作为联盟链的组织和节点之一，区块链版权存证所有信息均即时同步至公证处，保证任何时刻均可出具公证证明，具有最高司法效力。国家授权中心提供可信时间戳。区块链版权服务包括版权存证、版权检测追踪、侵权存证和版权资产共享四部分。

- 版权存证：将通过哈希算法计算出的存证数据指纹写入区块链，并根据用户需求生成

存在证书供用户保留，也可根据用户需求，提供纸质书面报告。在客户需要对存证的指纹进行验证时，提供数字指纹比对查询。

- 版权检测追踪：根据版权作品的内容特性，生成 DNA 特性，并将其在联盟链上进行登记；提供重点网站自动化爬虫，将监测到的内容与作品 DNA 进行匹配，相似度达到阈值自动进行侵权预取证操作；对已进行侵权预取证的内容进行持续追踪及进一步分析匹配，待确认侵权则直接进行侵权取证。
- 侵权存证：当发现侵权行为时，快速调用版权服务中的侵权取证接口，对侵权网站进行页面抓取取证，并将取证结果保存在版权平台中；将侵权行为固化为证据进行保存，数据永久存储且不可篡改，且具有法律效力。对于已进行侵权存证操作的侵权内容，版权服务提供持续性的侵权监控、侵权追踪等服务，确保侵权方对于侵权内容采取相应处理。
- 版权资产共享：版权资产共享平台在明确数字资产的所有者后，对于相关资产的运用做到可追溯性，安全性得到保障；版权的交易和存证相结合，实现内容消费的收益在原创作者和相关机构之间公平分配。

该方案有效地利用区块链的独特特性，具备以下几方面的优点：

- 安全可信：引入基于数字证书的身份标识，基于中心化的 PKI 体系，将版权局、公证处、内容平台等生态参与方作为参与节点上链，保证各方在区块链上进行安全、可信的协作。
- 实时登记：创作即确权，能够快速与公证等节点进行确权信息的确认，并实时、安全、可靠地保存在区块链上，设立多节点备份机制；便于第三方进行查证，其不可篡改的特性也保证了信息的安全可靠。
- 公平公正：引入区块链浏览器模块，提供链上信息查询服务，将所有版权确权、侵权存证等数据公开，任何个人和机构均可进行查询，确保服务公平、公正、公开，促进行业健康成长。
- 统一业务平台：任意节点都能完整备份链上节点信息，原创作者和相关机构共同维护统一业务平台，有利于便捷管理和公平透明地划分内容消费收益。

10.4 区块链存证和数字版权面临的机遇和挑战

区块链为困难重重的中国版权保护事业带来新的解决思路。展望未来，区块链版权既面临机遇，也面临不小的挑战。

10.4.1 区块链存证和数字版权面临的机遇

首先，中国政府积极扶持区块链技术的发展及其向文化产业的渗透。《“十三五”国家信息化规划》将区块链作为重要战略方向加以明确；中央网信办、文化部等文化产业相关职

能部门也公开倡导区块链版权的应用,认为区块链在知识产权保护领域会有很广的应用前景。

其次,迅速的中国数字文化产业和区块链产业将为区块链版权提供巨大的市场需求。数据显示,截至 2017 年 12 月,我国网民规模达 7.72 亿人,手机网民规模达 7.53 亿人,网络游戏用户规模 4.17 亿人,网络文学用户规模 3.53 亿人,网络直播用户规模 3.44 亿人,网络视频和网络音乐用户规模均超过 5 亿人,而从产值上讲,我国网络版权产业整体产值突破 5 600 亿元,我国区块链市场规模到 2020 年可达 5.12 亿元。

再次,民众付费意识和付费商业体系不断增强,为区块链构建版权付费体系创造了良好的社会氛围和消费环境。《2017 年中国网络新媒体用户研究报告》表明,33.8% 的新媒体用户已经产生过内容使用付费行为,15.6% 未付费用户有付费意愿,《2017 年中国网络版权保护年度报告》显示,2017 年我国用户数字内容付费规模达到 2 123 亿元,同比增长 28%;可见,中国网民的版权付费意识已大大改善。

10.4.2　区块链存证和数字版权面临的挑战

第一,付费商业模式和付费意识不健全是对区块链版权应用的极大挑战。数字时代信息大爆炸,知识产品资源、传播资源相对于人们有限的注意力而言已不再稀缺,吸引用户关注和流量反而成为有使用价值和交换价值的事,电视台、视频网站免费提供资讯娱乐节目供用户观看,这些机构的商业模式就是通过免费的内容来吸引用户,然后把用户,确切地说是把用户的注意力作为流量卖给广告商,从而用广告费覆盖各种开支、实现盈利;这种独特的商业模式已经在数字时代得到普遍应用,在这种环境下资源稀缺性能带来最大的价值。

第二,区块链本身的技术成熟度也会制约其应用规模。区块链技术自 2008 年诞生至今不过 10 年时间,虽然其技术潜力有望催生颠覆性力量,但它目前还处于研发布局阶段,许多技术风险和难关如性能、隐私保护和可扩展性还有待攻克,也没有形成全国范围的统一的技术标准和规范,这对于区块链及作为其细分应用的区块链版权来说,是能成功获得商家和消费者认可,获得商业成功的一大障碍。

第三,现有法律体系对区块链价值的认可和兼容是区块链版权能否深入发展的关键。版权制度从其诞生之初就是用以调节私人权益与公共利益的一种机制,如果不能与其他法律的、政策的、经济的、社会的、人文的因素相匹配,即使区块链版权具有技术优势,也没有发挥潜力的空间。侵权是非常复杂的利益纠葛,需要结合法律、经济、技术和社会等整合手段来解决,不能只指望区块链在工具处理层面来完全解决。

可喜的是,目前在法律层面区块链应用到数字版权有了两个积极的事件:

首先,最高法院出台司法解释,认可区块链固定证据的“真实性”。《最高人民法院关于互联网法院审理案件若干问题的规定》(以下简称《规定》)已于 2018 年 9 月 3 日由最高人民法

院审判委员会第1747次会议通过,自2018年9月7日起施行。《规定》第十一条提到,当事人提交的电子数据,通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证,能够证明其真实性的,互联网法院应当确认。这是我国首次以司法解释形式对区块链技术电子存证进行法律确认。

其次,2018年6月28日,杭州互联网法院首次确认区块链电子存证的法律效力,这也被认为是我国司法领域首次确认区块链存证的法律效力。该案件中,原告证明被告在其运营的网站中发表了原告享有著作权的相关作品。区块链系统通过第三方存证平台,进行了侵权网页的自动抓取及侵权页面的源码识别,并将该两项内容和调用日志等的压缩包计算成哈希值上传至区块链中,并以此作为提交法庭的证据。杭州互联网法院审理后认为,这一电子数据通过可信度较高的自动抓取程序进行网页截图、源码识别,能够保证来源真实。采用符合相关标准的区块链技术对上述电子数据进行了存证固定,也确保了电子数据的可靠性;在确认哈希值验算一致且与其他证据能够相互印证的前提下,该种电子数据可以作为本案侵权认定的依据。

杭州互联网法院相关负责人表示:对于采用区块链等技术手段进行存证固定的电子数据,应秉承开放、中立的态度进行个案分析认定;既不能因为区块链等技术本身属于新型复杂技术手段而排斥或者提高其认定标准,也不能因该技术具有难以篡改、删除的特点而降低认定标准,应根据电子数据的相关法律规定综合判断其证据效力。

中国银行法学研究会理事肖飒在接受采访的时候表示:"《规定》出台说明我国司法领域对于'证据'的态度开放,区块链作为一种'分布式存储技术'具有不可逆、不可篡改等特性,对于固定证据的'真实性'可以起到重要作用。但是,我们必须理解,虽然区块链技术本身对固定证据有优势,但真实世界里发生的事件,不能单纯依赖区块链技术,例如航空保险理赔纠纷。是否发生空难本身很难被区块链完整记录下来,很多时候是'人为'地记录在链上触发'共识机制',因此,在证明某一行为是否真实发生时,还是需要传统的书证、电子数据、物证等。""同时,《规定》提及区块链'入证'优先在互联网法院适用,这是对应了互联网法院的案件类型,在互联网上发生、履行完毕,这样就避免了前述保险纠纷的类似问题,从而大大增加了区块链技术证明事件真实发生的可能性,我们判断,受此利好影响,未来在区块链创业领域,针对证据研发的课题会越来越多,创新和创业也会相应增加。"

10.5 本章小结

文化是社会进步和发展的基础,在互联网时代,各种数字作品包括视频,电子文章、网络新闻等是文化的主要载体,数字作品在互联网中能快速地复制和传播,使人们获取知识和文化的门槛大大降低,这极大地促进了文化的传播和发展。但是数字作品这种特点也使传统的版权保护方式如专利申请、著作权登记等遇到非常大的挑战,数字作品的版权保护也无法得

到有效的保护,如果不能有效地解决这个问题,将会形成创造难且无法保证利益、盗版容易又能获得暴利的恶性循环,极大地降低人们的创作热情。本节系统地介绍了如何通过区块链技术解决数字作品的存证和版权保护难题,也介绍了业内该领域的解决方案。也介绍到目前区块链面临的挑战和机遇以及法律界已经开始解决其中最大的挑战,即如何让法律认可区块链在存证和版权保护方面的价值。笔者相信,区块链技术是解决数字作品存证和版权问题的有效途径之一,未来价值巨大,但需要较长时间技术和法律实践的积累。

第 11 章

能源领域应用案例

11.1 业务场景

近年来,全球能源需求增长缓慢,能源转型推动新能源快速发展,能源消费结构清洁化趋势明显。在新政策下,我国的能源需求增长速度每年稳定下降。能源消费构成中,煤炭和石油等传统能源占比下降,天然气、水电、核电和风电等能源供给一直在稳步增加。然而我国能源供给结构依然存在大量问题,包括供给垄断、结构转变缓慢、清洁化不足、价格非理性和供给动力不足等。

2015 年,国务院印发《关于积极推进"互联网 +"行动的指导意见》。关于能源电力,该《意见》提出:"通过互联网促进能源系统扁平化,推进能源生产与消费模式革命,提高能源利用效率,推动节能减排。加强分布式能源网络建设,提高可再生能源占比,促进能源利用结构优化。加快发电设施、用电设施和电网智能化改造,提高电力系统的安全性、稳定性和可靠性。"

1. 推进能源生产智能化

建立能源生产运行的监测、管理和调度信息公共服务网络,加强能源产业链上下游企业的信息对接和生产消费智能化,支撑电厂和电网协调运行,促进非化石能源与化石能源协同发电。鼓励能源企业运用大数据技术对设备状态、电能负载等数据进行分析、挖掘与预测,开展精准调度、故障判断和预测性维护,提高能源利用效率和安全稳定运行水平。

2. 建设分布式能源网络

建设以太阳能、风能等可再生能源为主体的多能源协调互补的能源互联网。突破分布式发电、储能、智能微网、主动配电网等关键技术,构建智能化电力运行监测、管理技术平台,使电力设备和用电终端基于互联网进行双向通信和智能调控,实现分布式电源的及时有效接入,逐步建成开放共享的能源网络。

3. 探索能源消费新模式

开展绿色电力交易服务区域试点,推进以智能电网为配送平台,以电子商务为交易平台,融合储能设施、物联网、智能用电设施等硬件以及碳交易、互联网金融等衍生服务于一体的绿色能源网络发展,实现绿色电力的点到点交易及实时配送和补贴结算。进一步加强能源生产和消费协调匹配,推进电动汽车、港口岸电等电能替代技术的应用,推广电力需求侧管理,提高能源利用效率。基于分布式能源网络,发展用户端智能化用能、能源共享经济和能源自由交易,促进能源消费生态体系建设。

4. 发展基于电网的通信设施和新型业务

推进电力光纤到户工程,完善能源互联网信息通信系统。统筹部署电网和通信网深度融合的网络基础设施,实现同缆传输、共建共享,避免重复建设。鼓励依托智能电网发展家庭能效管理等新型业务。

能源互联网即是基于互联网技术应用发展背景下的清洁、高效的能源利用方式,在缓解环境污染问题的同时,得以提高资源利用效率以及资源整合重组进程,有助于有效地进行能源供给侧改革。

国家政策鼓励新能源应用,对于生产新能源的企业可提供减少税收或直接提供补贴的优惠政策。其中国家对风能、光伏和生物质等可再生能源发电的上网电价均有一定程度的优惠,各地政府也对新能源发电进行补贴。

11.2　行业现状和业务痛点

1. 消费者缺少选择导致用电成本高

在能源领域,传统上是通过公共的电力公司(也就是提供电力的中央电网)完成电力能源交易,以净耗电量来计算电费,消费者没有任何选择权。因此导致公共事业费用很高,这些费用基本上都是来自于用户在市场上的能耗支付所得。

尽管现在涌现出很多新能源发电手段,如太阳能电池板,风力涡轮机等,但这些能源生产方法缺乏适当的基础设施和技术来储存多余的能源。在没有合适的生产分配手段的情况下,生产者也只能将产生的多余能量卖回电网,而不是直接卖给他的邻居。因此,电力的终端消费者在形成价格时并没有真正的发言权,他们无法真正选择所使用的能源来自哪里,以获得最高性价比。

2. 分布式电网管理控制困难

随着新能源发电手段的普及，现在越来越多的家庭都装上了自己发电、储能的家用设备（比如屋顶光伏、特斯拉 Powerwall）。而海量的分布式的小型发电端，中心化电网是管不过来的。多余的电力如何就近卖给社区用户，而不用再经过中心化电网与高损耗远距离传输成为一个需要解决的问题。

3. 碳资产开发流程不透明

2014 年，联合国政府间气候变化专门委员会发布报告，以超乎寻常的强烈用词，警告全球必须在 2100 年之前把温室气体排放减少到零，否则恐将引发生态和社会灾难。2015 年 12 月 12 日，《巴黎协定》在巴黎气候变化大会上通过，该协定为 2020 年后全球应对气候变化行动做出安排，主要目标是将 21 世纪全球平均气温上升幅度控制在 2℃以内，并将全球气温上升控制在前工业化时期水平之上的 1.5℃以内。

减少温室气体排放成为全球各国的统一目标，而碳排放的监控和交易即成为实现这一目标的重要手段。但碳排放的每项技术和政策途径都依赖于在全球市场中准确测量、记录和跟踪各个控排企业的碳排放数据、配额和 CCER 的数量、价格，以及数据的真实性和透明性。然而传统方法的透明度有限，标准不连贯，监管制度不统一，还存在严重的信任问题。中心服务器无法对数据安全做到绝对的保障，而信息的不透明也让很多机构和个人无法真正参与进来。碳资产开发流程时间很长，涉及控排企业、政府监管部门、碳资产交易所、第三方核查和认证机构等，平均开发时长超过一年，而且，每个参与的节点都会有大量的文件传递，容易出现错误，影响最后结果的准确性。

此外，国家政策鼓励新能源应用，对于生产新能源的企业可提供减少税收的优惠政策。随之带来的一个挑战是，企业是否如实上报所生产新能源的数量？是否存在非新能源发电“骗补”的问题？如何追踪溯源新能源的交易？

11.3 区块链解决方案及其价值和优势

2018 年 3 月，华为云与招商新能源合作，为深圳蛇口 3 个光伏电站实现基于区块链 FusionSolar 的智能光伏管理系统，提供清洁能源发电数据溯源和点对点交易系统。通过区块链技术实现可信交易和价值转移，利用多方共识和不可篡改特性达成点对点交易，实现清洁能源创新盈利模式，打造新能源交易信任基石。

该能源区块链关注发电端和用电端，充分发挥了区块链技术的可追溯和去中心化等特性，定点为社区提供清洁能源。在上述能源区块链项目中，将其位于蛇口的分布式电站每日所发出的清洁电力放入能源互联网平台，华为提供电站数据接入的技术支持工作。用户可以直接在平台上选择使用清洁能源或传统能源，当用户选择清洁能源时，区块链技术根据智能合约直接配对电站与用户之间的点对点虚拟交易，同时第三方认证机构将为用户出具权威电

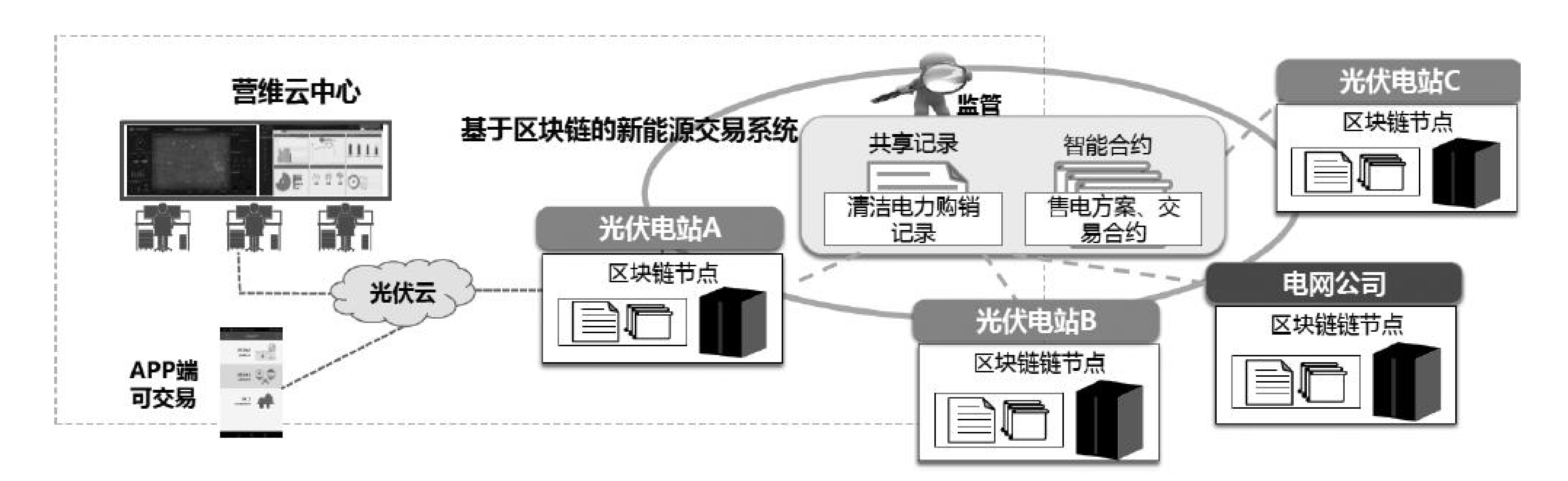


图 11.1 基于区块链的新能源交易系统

子证书，证明其所使用的是清洁能源电力。

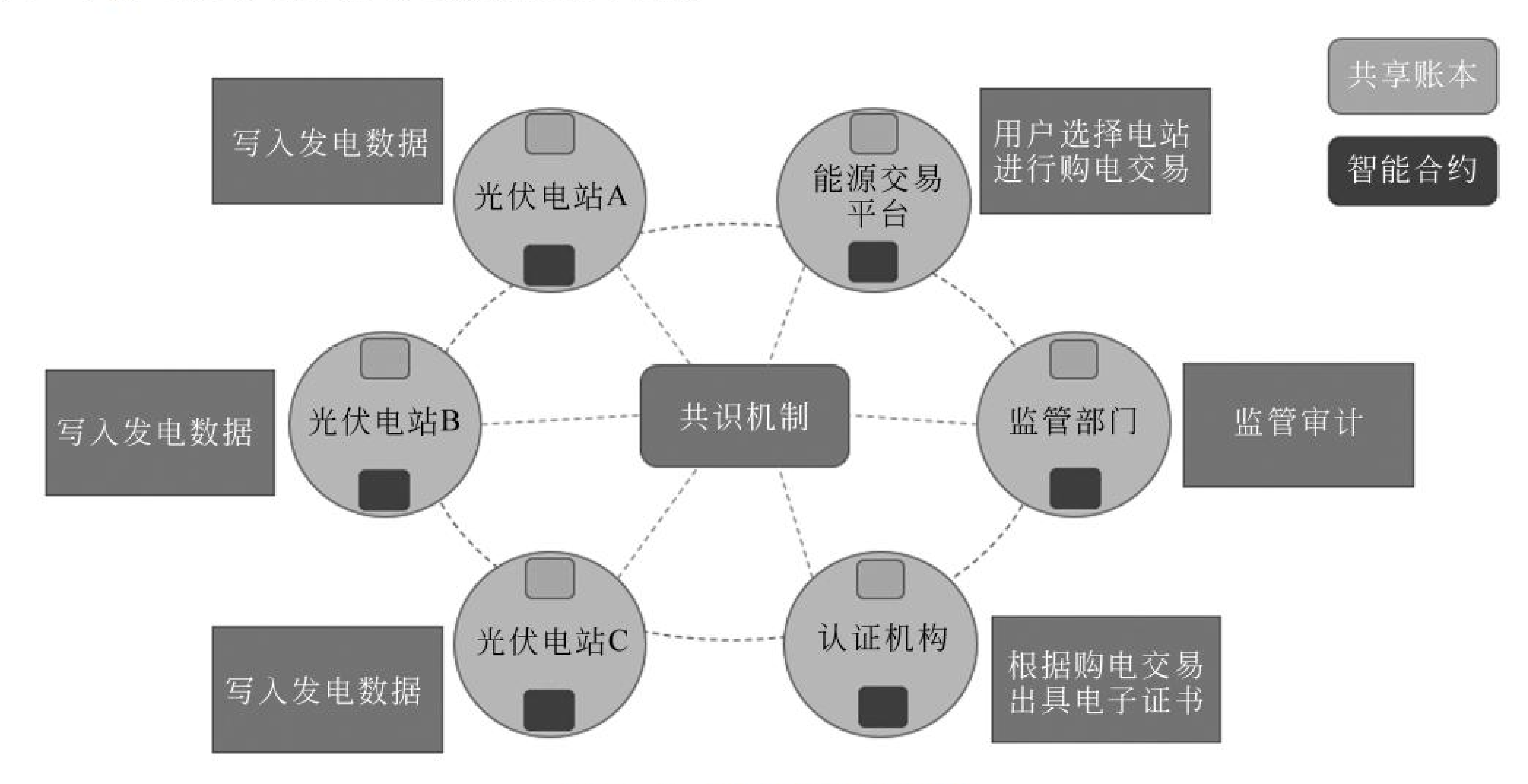


图 11.2 联盟链的组成成员

清洁能源电力认证等环境资产原本有着识别和认证困难的问题，区块链的不可篡改特性让其成为解决这类问题的关键。清洁能源电力的产生及消费可以直接用区块链技术进行记录，使得后续无论是电力生产者向政府申请新能源发电补贴或电力消费者进行碳证交易都既可信又方便。

区块链技术在能源互联网领域有如下应用价值：

1. 不依赖第三方的去中心化交易平台

很多年前曾经有人这样幻想未来的电力布局：人类已经不再需要通过大型电厂远距离将电输送到每家每户，而是可以通过太阳能电池板，由地方居民自己生产电力，自己使用。人类将同时充当着电力的生产者、销售者和消费者三种角色，实现“隔墙售电”。

应用区块链技术可以提供一种完全去中心化的能源系统，能源供应合同可以直接在生产

者和消费者之间传达,还可以规定计量、计费和结算流程,这样有助于加强个人消费者和生产者的市场影响力,并使消费者直接拥有购买和销售能源的高度自主权。这意味着,能源生产者不需要通过公共的电力公司(也就是提供电力的中央电网)就能完成电力能源交易。那些拥有能源生产资源(比如太阳能电池板)的公司,也可能将能源出售给社区。而对于消费者,相比于从中央电网购买电力,P2P 能源销售的优势在于有更大的选择权,价格可能更加便宜。另外值得一提的是,在能源互联网中,即便用户没有生产能源的技术,也能选择绿色可再生能源电力。

2. 利用智能合约实现电网分布式管理

对于分布式能源的管理只有一种办法:把电网变成分布式的、高度灵活自治的网络,这与区块链的结构是很匹配的。分布式能源可以增加电网灵活性,降低运营成本,提高可靠性。在区块链技术和智能合约的帮助下,可以有效地控制能源网络。智能合约将基于预定义规则向系统发出信号,制定如何启动交易的规则,确保所有的能量和存储流都是自动控制的。分布式能源正在缓慢改变配电系统与大容量电力系统的作用,这些变化可以改变电力传输和电网运营商对各种运行条件的响应。区块链可以将可再生能源和其他分布式能源添加到电力系统中,提高分布式能源的可视化和控制性,以满足日益复杂的电网运营需求。智能合约允许供应商和消费者能够通过创建基于价格、时间、地点和允许的能源类型等参数实现销售自动化。理论上,基于区块链的分布式电网控制管理可以创建更优的电力供需平衡。

3. 碳资产/新能源交易环节简化及端到端透明化和防篡改

在碳跟踪与注册的应用场景中,区块链的核心能力与围绕开发、部署和管理排放跟踪与交易系统的诸多挑战保持一致。作为交易数据的可信存储库,区块链可用于简化交易,加强验证过程,并消除对集中管理的需求。区块链用于碳跟踪与注册的另一个好处是有机会创建不可更改且透明的市场数据记录,可以为全球的碳库存和注册管理机构提供清晰度、可信度和互操作性,有助于在碳捕捉、利用和储存活动等方面跟踪碳排放。

将新能源的生产交易数据分散地存储在一个区块链上将有可能保持所有能量流和业务活动的分布式安全记录。由智能合约控制的能量和交易流可以以防篡改的方式记录在区块链上。监管审计部门能够从区块链上获得真实可靠的数据,防止"骗补"的行为。

11.4 能源区块链应用面临的机遇和挑战

目前对于绝大部分地区来说,相对于中央电网,点对点的电力交易在供电安全和稳定性上都还有欠缺。在缺乏规模效应的情况下,甚至于很多项目在价格上也不具备优势。

其次,去中心化的区块链只能省去电力交易的中介费用,而能源公司对用户进行的所有能源服务都是天然中心化的,这部分的费用并不能省去。

另外,由于电力是我们人类所有生产生活的基础和动力,所以电力行业一直都会是一个

政策强监管行业。供电安全、供电质量、供电稳定对于整个国家的发展是重中之重。比如纽约政府不允许个人售电，所以供方和需方点对点直接交易的方式本身还依赖政策上的转变。

11.5　本章小结

能源这个传统重型行业是一个涵盖范围十分广阔的领域，区块链技术具有深厚而实际的应用基础，本章中所描述的应用场景也只是目前在该领域进行探索的一小部分，其他应用场景还包括新能源汽车充电、去中心化能源交易、能源代币等。如同区块链在各行各业慢慢渗透一样，我国在能源区块链领域现在还是一片蓝海，但近年来也有越来越多的开拓者加入了进来，在变革中寻找发展机会。在这一场变革中，从传统巨头到新兴创业公司都没有缺位，随着越来越多的应用场景落地，必将对能源领域诸多方面产生广泛而深远的影响。

第 12 章

区块链应用的判断准则

经过前面章节的介绍,读者对于区块链自身具有的分布式、去中心化、去信任、不可篡改、可编程等特性都已经熟悉,并且经过对区块链涉足的领域如金融行业、供应链/物流、政务服务、存证及版权、能源领域等进行的分析,相信读者对区块链的颠覆性价值以及应用趋势都已经有了深入的了解。实际上区块链的潜力和价值远不止如此,还有很多其他的行业和应用迫切等待我们的挖掘和发现。此时,我们会发现前面介绍的行业和应用都是区块链先驱们根据自己丰富的从业经验,结合区块链自身的价值特点进行发掘和提炼的,现在让大家自己去判断一个区块链适用的场景,往往都会感到无从下手。本章就以此为出发点,给大家提供一个判断区块链应用的简单易行的思路和方法。

区块链面向行业的解决方案,需要多方参与,构建行业联盟,形成事实标准,抢占第一波市场。区块链适用于多状态、多环节,需要多参与方协同完成,多方相互不信任,无法使用可信第三方(Trusted Third Party,TTP)完美解决的事情。我们可以采用图 12.1 所示的流程图来判断一个场景是否需要区块链。

图 12.1 展示了一个较为严格的区块链应用判断流程,目的是给大家提供一个快速识别区块链应用的方法,但很多场景下这些约束条件可以进一步放宽。下面将对流程中的每个步骤进行一下简单的阐述,方便大家理解。

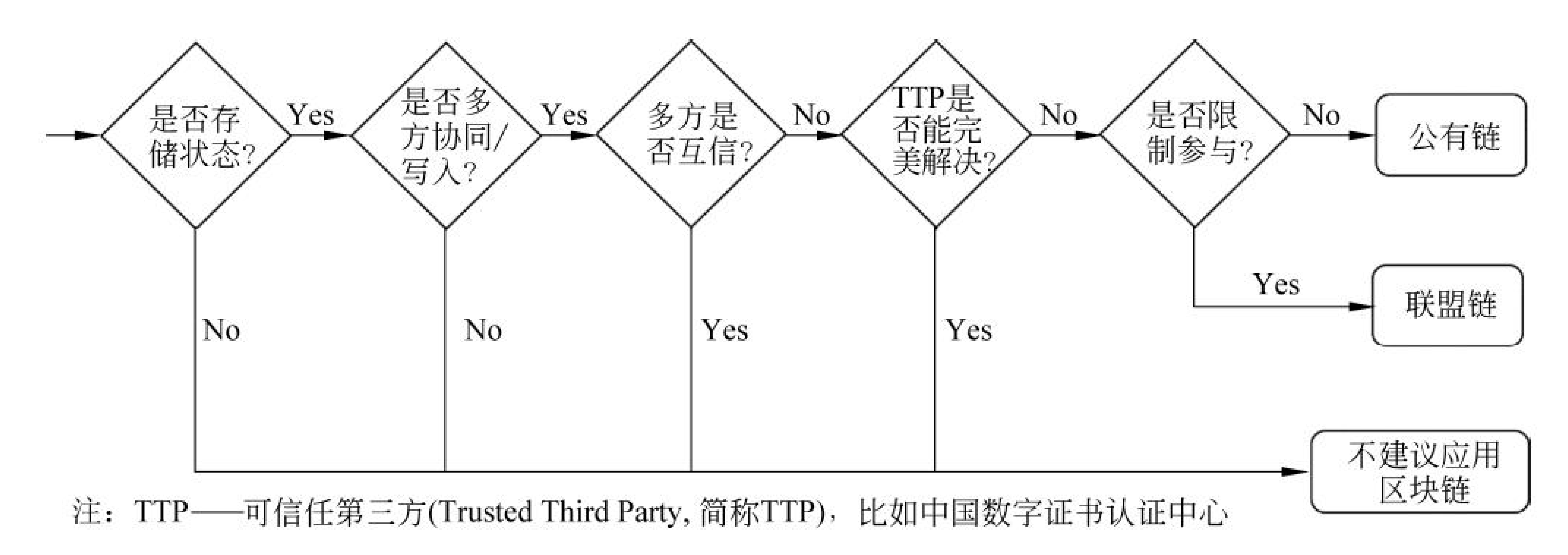


图 12.1　判断某场景是否需要区块链

12.1　准则一：是否储存状态

我们可以将区块链通俗地理解为一个分布式的数据库，使用数据库的各方都可以存储交易数据，我们把存储的数据称之为"状态"。区块链又经常被称为"账本"，既然是账本，那么最重要的用途就是记账，记录每笔交易的重要数据，以便将来以此作为查账和避免纠纷的依据。根据前面章节介绍的区块链的结构也很好理解，区块结构中最核心的部分就是用来存储交易的信息(状态)，因此可以说没有状态存储就不会有区块链。需要注意的是，这里的交易指的是广义的交易，并不限于货币和金融的交易，一切会产生数据状态变化的事务都称之为交易，例如：账户的创建、商品信息的变化，甚至对于一次查询的审计信息的记录等都可以算作交易。

这里有一个需要注意的问题是：业务需要保存的数据很多，到底什么样的数据适合用区块链来存储？鉴于应用的多样性以及用户需求的不确定性，这个问题其实并不容易回答，但是我们仍然可以从两个角度来试图缩小考虑问题的范围：什么样的数据不适合上链以及什么样的数据适合上链？

首先来看什么样的数据不适合上链。从业务角度看，不需要共享的数据不适合上链。例如用户的私钥，是用户绝对不想与其他人分享的信息，如果上链，就意味着私钥会被每一个参与者获取并存储，即便是被加密也会有泄漏的风险，因此没有必要上链。从性能角度看，过于庞大的数据和更新过于频繁的数据也不适合上链。例如用户上传的一些二进制的介质、音视频、日志文件等。因为区块上存储的数据作为链的一部分是会被永久保存并同步到每一个参与节点用来保证完整性的，如果存储的数据过于庞大，则会严重影响同步性能，占用有限的存储空间。另外由于当前区块链的交易需要通过密码学算法进行哈希和加解密的签名运算，交易的最终数据也需要通过共识算法进行排序才能最终落块，在性能上还有一定的限制，因此过于频繁的写入操作还不太适用区块链。

那么什么样的数据适合上链呢？简单来说就是需要共享的、需要具备可信度、不能被篡

改并且需要可追溯的数据。例如保险行业的保单信息,用户签署了什么样的保险协议,需要被妥善保存,将来出险的时候必须以此为依据进行理赔,因为不可篡改,保险公司无从抵赖,也因为可以共享和追溯,一旦产生纠纷也可以由监管部门追溯取证。再如能源行业,如果使用区块链来记录电量的交易,那么拥有光伏发电的家庭就可以和需要用电的家庭进行自由交易,每一笔电量的产生和去向都有清晰的历史被区块链记录在案,不能篡改,同时支持发电方和用电方进行查询和追溯,哪家发了电,哪家用了电,交易清晰无法抵赖,避免了纠纷,是使用区块链的合适场景。

此外说到状态存储,就不得不提及信息安全,这也是当前区块链大规模普及的障碍之一。我们都知道区块链之所以难以篡改,就是因为每一个参与交易的节点都拥有完整的区块链账本数据,可以对任何交易或账户状态进行验证。但是这样也带来一个严重的安全问题,就是区块链账本数据对所有人公开了,而在很多场景下,这样的做法是难以被接受的。拿货币转账的交易举例来说:用户 A 一开始在系统中存入了一定金额的货币,用户 B 也存入了一定金额的货币,随后用户 A 向用户 B 进行了一定金额的转账,因为用户 A 和用户 B 的余额都存储在区块链上,智能合约的逻辑可以验证用户 A 的余额大于转账金额,并且把交易结果写回到区块链上,对用户 A 和用户 B 的余额进行更新,最终这笔交易写入新生成的区块中后,区块会被同步到用户 A 和用户 B 相关的节点上,他们都可以查询到这笔交易以及自己当前账户的余额。但是很多情况下,作为用户来说,并不希望自己的余额被其他用户看到,作为交易的双方也不希望交易的详细信息被第三者读取到,那么这个问题如何解决呢?一般情况下我们可以使用前文提到的同态加密的技术来解决这个问题。

同态加密就是智能合约在存储用户的余额状态到区块链上时,存储的并不是明文,而是使用相应用户非对称密钥的公钥通过同态加密算法加密之后的数据。在同态加密交易过程中,转账双方的余额都没有经过解密,并且交易记录存储到区块链上之后只能被交易双方解密查看,第三方只能看到密文,无法解密。这样既达到了区块链无法篡改、可以被追溯和监控的目的,又能保护用户隐私不被泄露。同态加密技术细节前文已经有详细介绍,就不在此赘述了。

12.2 准则二:是否多方协同写入

是否存储状态只是判断流程的第一步,其次还要依据是否多方协同写入来进行判断。前面一直提到区块链一个突出的特点就是去中心化,而多方协同写入才能够将区块链这种特点的优势完美地发挥出来。有人曾经说,区块链颠覆的核心就在于去中心化,我们现在的世界存在了太多的中心化系统,然而这些中心化的系统却和用户日益增长的去中心化需求产生了矛盾。中心化系统有如下弊端:

首先是权力过于集中。中心化系统的一切数据的来源都是数据中心,数据中心拥有至高无上的权力,数据的存储逻辑全部由中心决定。正如人类社会中权力集中的地方必然存在腐

败一样,数据权限集中的地方也容易滋生“腐败”,当然这个腐败指的是对数据的篡改。由于只有一套中心化的系统,如果没有额外的监督审查机制,数据可以很轻易地被篡改。但是构建一套监督审查机制也是十分复杂的,到底由谁来监督?监督的部门有没有公信力,是否被信服?这些都是问题。

其次是集中的数据难以使用。数据中心化,意味着任何使用数据的单位或者个人都要从数据中心获取数据,这种数据同步模式有两个问题:其一,随着使用数据的部门增多,给数据中心带来极大的数据访问压力,数据中心会形成数据访问的性能瓶颈,这对数据中心的性能和扩展性提出了极高的要求。其二,新的部门想使用数据必须和数据中心进行对接,无形中增加了数据使用的成本,给数据的扩散造成了障碍,极大地影响了数据价值。前些年我国正处于数字化转型的初期,大量数据由纸质数字化转化而来,但是各地又形成了一个个数字孤岛,各省市之间的数据不能同步,给政府部门的工作造成了极大困扰。比如,小轿车跨省违章不能及时被追责,因为违章的信息不能及时同步到其他省市。再比如,有些公民从一个省市移居到另外省市,重新办理了新的身份证,有时候会出现一个实体个人有两个合法身份证号的情况,也是因为各省市身份信息不能及时同步的原因。其实并不是政府部门不作为,而是进行这样的数据同步需要同时拉通各省市很多部门、调动很多资源、成本过高而已。

最后是集中的系统抗攻击能力差。数据集中意味着黑客只要攻陷了一个数据中心,就得到了全部的数据权限,可以为所欲为。而防护部门必定绞尽脑汁花费高额成本进行防范。这样做不仅提高了成本,还只能在一定程度上降低风险但又不能彻底消除。

以上这些中心化系统的弊端,我们都可以依靠区块链技术来解决,如图 12.2 所示,将数据中心化的账本转换为区块链的分布式账本。这样每个数据节点是对等的,拥有完整的数据链,黑客除非攻陷了大部分节点,否则不会影响数据的正确性。另外,各个节点之间也可以相互监督,真正实现数据自治。

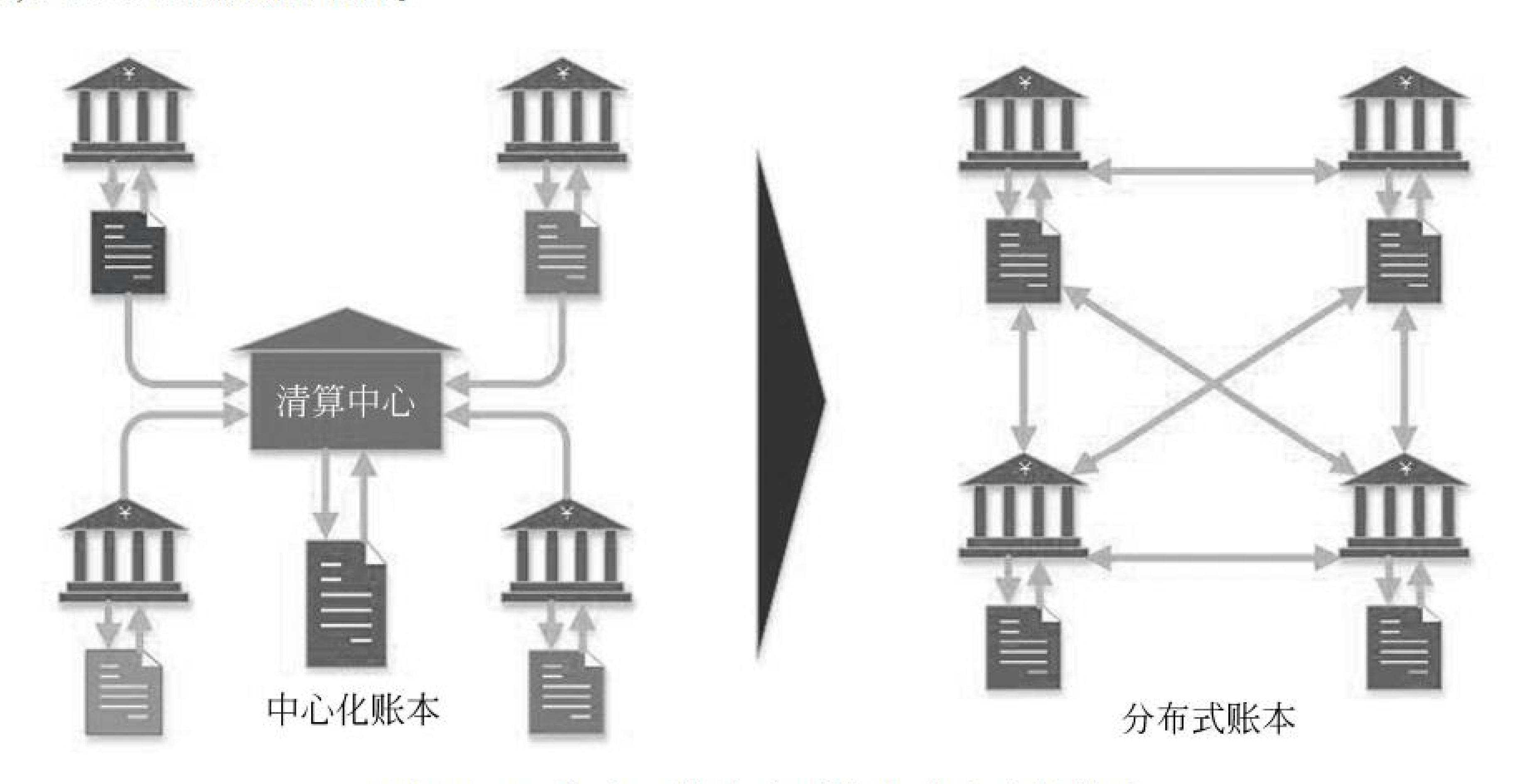


图 12.2　从中心化账本到分布式账本的转变

以电力系统为例,当前我国的电力系统还是一个中心化的体制,以前购电并不像现在这样简单,只根据一个用户编号就可以使用支付宝之类的互联网应用购买。因为只有电力部门才拥有对电卡读写的权限,在当时没有智能电表进行网上购电时,必须拿着电卡实物去电力部门排大队购电,并且办理过程十分冗长。后来出现的智能电表可以算是借着互联网将中心化系统进行了一次很好的升级,互联网通过网络将电力系统延伸到各家各户。但是,互联网只改变了网络连通的现状,将数据传播到各家各户,却没有改变系统的权力中心化状况,将权力转移到用户手中,用户依然需要使用电力系统对电卡进行读写,也就是电力部门垄断了话语权。而在上面的例子中,用电家庭和发电家庭使用区块链来进行电能交易才算实现了区块链的真正价值。

由此我们不难理解,如果一个区块链只有一个写入者,那么无论拥有多少共识节点都是没有意义的,因为写入者可以随意写入、随意变更数据,本质上又变成了一个集中式的系统。因此,一个合理的区块链应用是要求参与的各方都可以具备预先规定好的写入权限,并且相互制衡,从而达到去中心化的目的。

12.3　准则三:多方是否互信

首先我们来谈谈关于信任的问题。互联网诞生之初,最先解决的核心问题是信息制造和传输。随着互联网的大规模发展,我们使用TCP/IP协议构建出来一条条网状的信息“高速公路”。在这个高速公路网上,我们能够将信息快速生成,并复制到全世界每一个网络所能够触及的角落,并且这种信息的传递是极为高效并且越来越廉价的。从此,我们进入了一个“信息爆炸”的时代,整个互联网上的信息开始以几何级速度增长。

然而,随着互联网进入我们生活的方方面面,我们却发现有些信息是无法传播和复制的,或者说传播无法很容易地进行。比如说货币支付,我们不能直接把要支付的钱复制到对方的账户上,必须要到银行柜台花个把小时排队进行办理,后来有了ATM机,我们仍然要出门乘坐交通工具花费很长时间办理。当然后来有了网上银行,有了U盾,但我们仍然离不开中心化的银行系统,依然有诸如转账需要花费不菲的手续费用、转账金额或许不能立即到账等一系列问题。产生这些问题的根源都是因为我们的互联网非常善于处理信息分享,而不能解决“价值传递”或者说“信任”这个事情。

多方是否互信也是判断应用是否适合区块链的一个重要指标。区块链的意义在于使得互不信任的各方可以通过区块链传递和获取信任,并且这种信任建立的成本是很低的,具有极高的性价比。如果参与写块、读块的各方是完全信任的,那么即便各方在物理上分散,在逻辑上也是集中的,这种场景下区块链的信任传递特性就失去了意义,因此并不适合使用区块链技术。但是我们注意观察就会发现,其实这些所谓各方的完全信任并不是天然具备的,大多数场景下是基于一定的信任机制的,这种机制有可能是基于自建的一套信息系统,也有可能是基于传统的可信任第三方(Trusted Third Party,TTP)。而这种信任的根基并不牢固,并且

都存在一定的弊端,因此,如果我们认真分析,这些应用和场景也都可以转化为区块链应用,并且能够从中获得很多好处。

综上所述,如果说区块链颠覆的核心在于去中心化,那么区块链与生俱来具备的互信特性就是去中心化的基础。没有互信作为基础,谈去中心化是毫无意义的。区块链利用密码学的哈希算法(Hash)和数字签名(Digital Signature)来保证交易的发起人无法被冒充,而区块的链式哈希结构则保证了历史交易被永久地记录,无法被轻易地篡改。区块链这一系列的特点给互联网带来了前所未有的互信的特性。如果说第一代互联网解决的是数据传递的问题,那么以区块链为基础的互联网解决的就是信任传递的问题。

12.4　准则四:TTP 是否能完美解决

可信任第三方(Trusted Third Party,TTP)是在第一代互联网无法解决互信问题的前提下的产物。当时随着互联网的日益膨胀,人们迫切希望在虚拟和现实世界中建立一种信任的关系,如果缺乏这种纽带,那么虚拟的东西永远是虚拟的,就不会出现今天百花齐放的电商和虚拟业务,也就不会有当今互联网的蓬勃发展。但是建立这种信任的纽带又是极其复杂和昂贵的,比如银行的在线业务和应用是需要银行以其强大的资金和政府公信力为其背书,提供对业务和纠纷的监管和决断。很多电商也是依赖于强大的资本来提供公信力和背书。其他更多中小企业并没有足够的实力和公信力来自建这种公信的系统,它们只能依赖强大的第三方提供信任的服务。从中我们可以看到,TTP 的最大缺点在于昂贵的高门槛、接入运营的复杂度高以及权力过于集中等弊端。权力集中就意味着腐败,就有被人为渗透的可能,同时集中的系统普遍抗黑客攻击的能力较弱。

而区块链天生的去中心化和可信的特性,恰恰是解决上述问题的最完美手段。因此,判断应用是否适用区块链一个很重要的标准就是 TTP 是否能完美解决当前的信任问题。如果 TTP 能完美解决,那么确实没有上区块链的必要。需要注意的是,当前很多看似用 TTP 解决的信任问题其实解决得并不完美,例如电商和用户之间的纠纷,公信部门系统自身故障以及受到攻击产生宕机的事情也时有发生。因此,我们在判断应用是否适合使用区块链的时候,并不是判断 TTP 能否完美解决信任问题,而是 TTP 的缺陷我们能否接受,TTP 的成本能否接受。

12.5　准则五:是否限制参与

判断流程至此其实已经基本确定应该适合使用区块链了,是否限制参与这一指标只是用来判定我们的应用到底适合公链还是联盟链。

公链对用户的准入要求并不高,比如所有的虚拟货币,基本上任何人任何机构只要进行简单的注册,生成私钥和证书即可参与。而联盟链则不同,比如金融业各银行之间的转账业

务，并不希望未经授权的人参与，是建立在一定的信任基础之上的，比如某几家银行形成了一个战略联盟，之间使用区块链同步一些信息。但是这些银行之间又不是完全信任的，只是因为之间的利益关系联系在了一起。在这种前提下，联盟链就比较合适。想加入的银行需要通过一系列流程方可获得参与区块链的资质，同时联盟区块链中的信任各参与方都能通过区块链不可伪造、不可篡改等特性进行相互监督。因此公链和联盟链并无好与不好之分，各自有适应的场景。

上述流程给出了一个简单易行的审视各类应用是否适用于区块链的基本方法，避免读者在面临陌生领域或全新行业进行区块链应用分析时无从下手。另外需要特别注意的是，本书中提到的五大判断是作为判断区块链应用的充分不必要条件，也就是说，如果满足五大判断准则就基本可以肯定为区块链应用，但没有全部满足的应用也很可能是区块链应用。在初次尝试使用这五大准则时，读者常犯的一个错误是将需要分析的场景严格按照这五条准则一一对号入座，必须全部满足准则才判定为适合区块链的应用，这样做是很不灵活的。在实践中，请读者根据实际需要，结合业务自身的特点以及企业的实际经验进行量身定制、灵活剪裁，方能发挥区块链的最大价值。

12.6 本章小结

本章针对区块链应用缺乏统一的判断标准，同时业界也缺乏足够的经验积累的问题，创新性地总结出了一系列区块链应用的判断准则，并对准则进行了逐条分析讲解和例证，非常适合新入区块链领域的业务分析人员作为手边工具对陌生新业务领域进行区块链适用性分析，甚至对一些经验丰富的区块链老手也有一定的理论化指导意义。同时，我们也强调了这些区块链准则和分析流程在使用时不必拘泥于准则的条条框框，要根据实际情况进行取舍补充、灵活运用，才能对业务是否适合应用区块链进行更准确的判断。

第 13 章
如何使用公有云区块链服务

13.1　公有云是区块链应用的最佳载体

区块链在近几年非常火热,也为企业及各大机构在许多领域的痛点提供了解决思路。众多企业开始着手构建企业内、企业间的区块链应用,政府部门也在主导构建行业、政府、公益等领域的区块链应用。然而对于企业及政府部门来说,开发、搭建一套区块链系统并非容易,区块链人才的缺乏、底层平台搭建的复杂及运维的烦琐,使得企业无法聚焦于上层应用的开发与创新。

云的开放性和云资源的易获得性,帮助公有云平台成为当前区块链创新的最佳载体。公有云是获得弹性资源和快速实现新技术架构的最佳途径。云环境中的区块链服务可以简化复杂组件的设置,而云基础设施和云平台服务也可以提升运营效率和降低早期投入门槛。

虽然从本质上来看,现在的公有云厂商提供的云计算资源,类似于传统的中心化服务,由各个云服务厂商提供存储、计算、网络等服务,看似与区块链的去中心化有矛盾之处,但是目前公有云已经可以提供多组资源隔离、混合部署、跨云支撑等能力,足以达到客户真正的去中心化诉求。区块链网络可以部署在不同可用区(AZ)之间,不同的联盟方拥有独立所属权的资源控制。同时,云计算的弹性伸缩能力,可以更好地为区块链应用扩缩容带来便利,按需使用,按量付费。

在公有云上搭建区块链网络,可以帮助企业节约投资、简化流程。首先,用户无须购买和维护 IT 基础设施。IT 基础设施投资往往会占用企业的很多开支,在机房选址、硬件采购、电

力成本等方面都需要大量的投资,硬件的折旧也会不断地消耗企业资金。其次,可以为用户节约区块链应用的维护成本。目前企业使用主流的区块链网络多来自开源社区,社区版本在可靠性、稳定性、满足度等方面都还不能支撑企业级的业务,因此需要投入大量的人力进行维护与开发。当社区版本更新迭代时,版本的适配升级也会带来大量的人力消耗,以及可能带来业务不稳定的风险。再次,可以降低人员使用门槛,减少人力成本。随着社区版本的不断升级,底层代码量也日益庞大,如何部署、调试需要专门的投入。当业务需要定制化功能时,很多时候社区版本无法满足,导致需要开发复杂的上层业务。例如:Web/IoT 端为了快速访问 Fabric 网络时,原生的 SDK 对系统的消耗比较高,设计应用时需要考虑这部分性能消耗。而不少云平台提供了基于 RESTful 的访问接口,将大大简化端侧业务开发。最后,用户可以按需购买服务,随用随买。在上层业务构建初期,一般无法准确地估算底层资源的实际消耗。如果业务大规模增加,采购硬件、扩容环境的人力、物力、时间的消耗,都会阻碍业务快速发展。而使用公有云则无需关心这些细节,企业客户按需购买资源,在业务初期可以购买少量的进行测试验证,当业务上量后,可以迅速扩容,业务减少时,也可以弹性减少资源占用,从而节约成本。

13.2 华为云区块链服务 BCS 初探

2018 年 2 月 1 日,华为云发布企业级区块链开放平台区块链服务 BCS(Blockchain Service),是基于开源区块链技术和华为在分布式并行计算、数据管理、安全加密等核心技术领域多年积累基础上推出的企业级区块链云服务产品,帮助各行业、企业在华为云上快速、高效地搭建企业级区块链行业方案和应用。将企业从烦琐耗时的区块链基础开发和部署中解放出来,使其聚焦有价值的上层应用,快速开发自身业务场景,不再让技术限制自身业务的想象力。如表 13.1 所示,华为云区块链服务 BCS 具备灵活高效、安全可靠、简单易用等特性。

表 13.1 华为 BCS 服务特性

特　　性	特性描述
灵活高效	支持多种高效共识算法选择 多角色节点和成员动态加入/退出 秒级共识(PBFT 5000TPS +/Kafka 10k + TPS) 采用容器化物理资源管理,极致弹性伸缩 支持线上线下混合部署 支持跨云(如华为云 + SAP 云)业务部署
安全可靠	20 + 全球权威认证,安全合规 完善的用户、密钥、权限管理和隔离处理 多层加密保障和国密支持 零知识证明和同态加密等隐私处理 可靠的网络安全基础能力,运营安全无忧

续表

特　　性	特 性 描 述
简单易用	基于 Hyperledger、kubernetes 搭建，配置简单，数分钟内即可完成部署，满足一键式部署区块链实例、一键式部署区块链解决方案 提供全流程、多维度的自动化运维服务 支持链码在线编译 首创区块链结合 MySQL 存储，显著提升账本查询性能 支持 RESTful 方式访问，满足 Web/IoT 等瘦客户端使用

华为云区块链服务致力于打造区块链生态，BCS 服务实现区块链的底层技术支撑，包括共享账本、安全隐私、智能合约等，同时提供区块链部署、运维能力。由行业合作伙伴构建领域通用解决方案，并提供咨询与开发服务，助力企业顺利实施区块链应用落地。

基于华为云，BCS 支持为企业客户构建全球范围的区块链价值网络，支持跨云对接，支持与华为云运维监控、大数据服务对接，提供全栈技术能力。图 13.1 为 BCS 服务在华为云上的整体架构，从图中可以看到华为云提供了完整的区块链应用的技术栈：从最基层的计算、存储、网络资源到中间的区块链平台的构建部署，以及最上层的用户业务应用领域都进行了非常全面的覆盖（区块链平台部分属于华为云区块链服务，业务应用部分由华为云其他服务提供支持，如云安全、人工智能、大数据分析等）。目前华为自身以及与相关合作伙伴提供了几大解决方案供企业选择，其他行业的在不断完善中，这些解决方案包括供应链金融、食品溯源、港口物流、积分交易、行业数据共享、税务票据、版权确权等。后面的章节对企业如何使用华为区块链服务进行简单介绍。

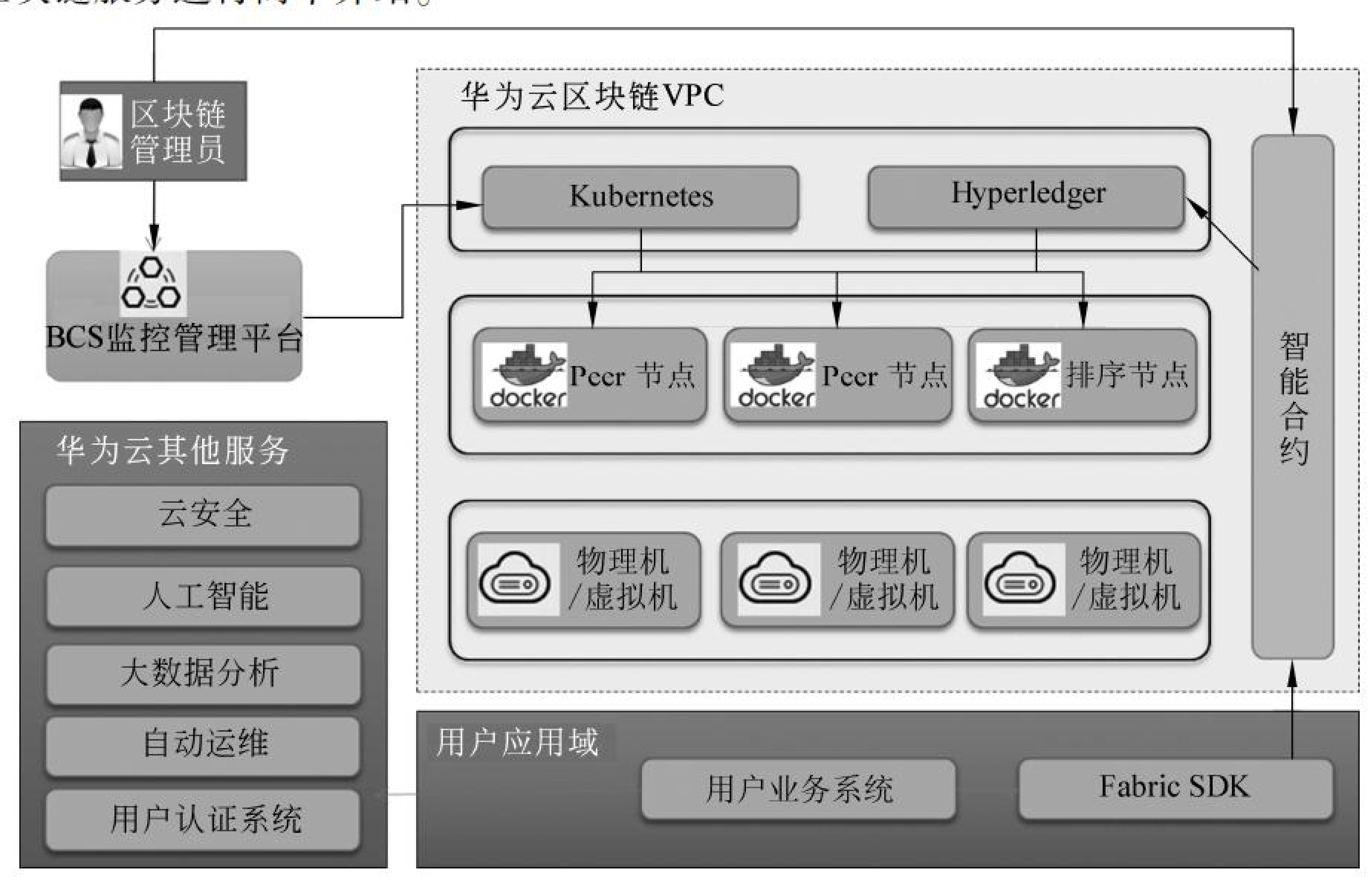


图 13.1　BCS 服务在华为云的架构

13.3 基于华为云区块链服务构建企业应用

前面的章节中提到过，BCS服务的诞生是为了帮助企业快速构建自身的区块链应用，企业具体如何实现区块链应用落地，如何判断业务是否适用区块链，如何进行区块链开发及部署，后续如何维护，本章节将会逐一展开进行介绍。

从图13.2所示的逻辑架构图可以看到，一个完整的企业区块链应用架构由上至下包含三层：业务应用层、合约层和底层区块链平台层，这三个层级决定了区块链应用开发的成本，是企业在区块链应用的决策、需求分析以及架构阶段需要着重考量的方面。



图13.2 华为云区块链服务逻辑架构

- 业务应用层

这一层是区块链应用的对外表现层，主要功能是对外提供友好易用的界面为企业用户提供业务服务，形式可以为一个Web应用或者一个手机移动端的APP。这一层和传统的Web应用以及移动端APP并无明显差别，对最终用户来说并不需要感知区块链的存在，只需确保区块链应用不要破坏用户一贯的软件使用习惯即可。在这一层次上，华为云区块链服务能够提供给企业的是一些工具类的帮助，例如：提供区块链链码的RESTful调用方式减轻应用层开发的难度和负担等。关于更多的与应用开发相关的内容，企业可以咨询华为云其他的服

务，比如华为云云容器引擎、微服务引擎等，这些服务不在本书的讨论内容之中，在此略过。

- 合约层

合约层顾名思义是智能合约的部署层，是企业应用使用区块链服务最重要的一层。智能合约封装了企业对区块链使用的全部业务逻辑，是企业业务精髓的体现，每个企业的智能合约都不尽相同，是需要每一个开发区块链应用的企业用心设计，定制开发的部分。基于其重要性，华为云也对合约的开发部署提供了有力的支持。首先，在智能合约代码的开发上提供了在线链码编辑器，让用户可以在线开发、编译及调试。其次，华为云提供了对链码的完整的生命周期管理，用户可以使用界面便捷地安装部署链码。最后，华为云还提供了丰富的链码样例、模板供开发者参考，将来还会提供更为通用的链代码类库以加速开发者开发链码的过程。

- 区块链底层平台

华为云区块链服务平台 BCS 以华为公有云服务为基础架构，除了为用户提供计算资源、通讯资源和存储资源以外，更进一步封装了区块链底层平台，将区块链记账能力、区块链运维能力和区块链配套设施能力转化为可编程接口，企业在开发时只需要关注应用层和合约层即可，极大地简化了区块链应用的开发过程，让开发者专注业务逻辑，提升开发效率。

13.3.1　区块链服务的交付模式

从交付的角度看，如何选择合适的商业模式进行业务落地是客户首先要考虑的问题。按照企业用户的诉求，华为云区块链服务解决方案提供三种交付模型：

Turnkey 模式（合作伙伴 + 华为云 BCS）：Turnkey 就是所谓的交钥匙模式，当企业有区块链诉求时，可以自己指定或者选择华为提供的第三方合作伙伴，由华为云解决方案专家参与，共同分析客户的业务诉求，根据业务的场景制定区块链解决方案，并由第三方合作伙伴完成业务的开发，交付最终的软件给客户。

企业 + 合作伙伴 + 华为云 BCS 的模式：此方案适用于企业自身需要参与一部分业务系统开发的情形，根据 BCS 生态系统划分，可由企业完成自身业务系统构建，由合作伙伴完成行业解决方案内的智能合约开发，由华为云提供区块链底层基础设施，共同搭建企业所需的业务系统，企业以最少的人力投入，快速构建区块链应用。

企业 + 华为云 BCS 的模式：当企业有较雄厚的技术储备、较强研发团队时，可以选择直接基于华为云区块链服务进行开发。华为云为企业提供咨询与架构服务，帮助企业分析区块链应用的解决方案，设计系统对接流程，并提供有力的技术支持和保障。

下面就带领读者体验一下如何快速构建一个简单的区块链应用。

13.3.2　区块链应用构建极速之旅

使用华为云开发企业区块链应用极为简单，只需六个步骤：业务场景分析、梳理上链信息、创建区块链服务、编写链码并部署、业务集成、区块链服务运维，如图 13.3 所示。

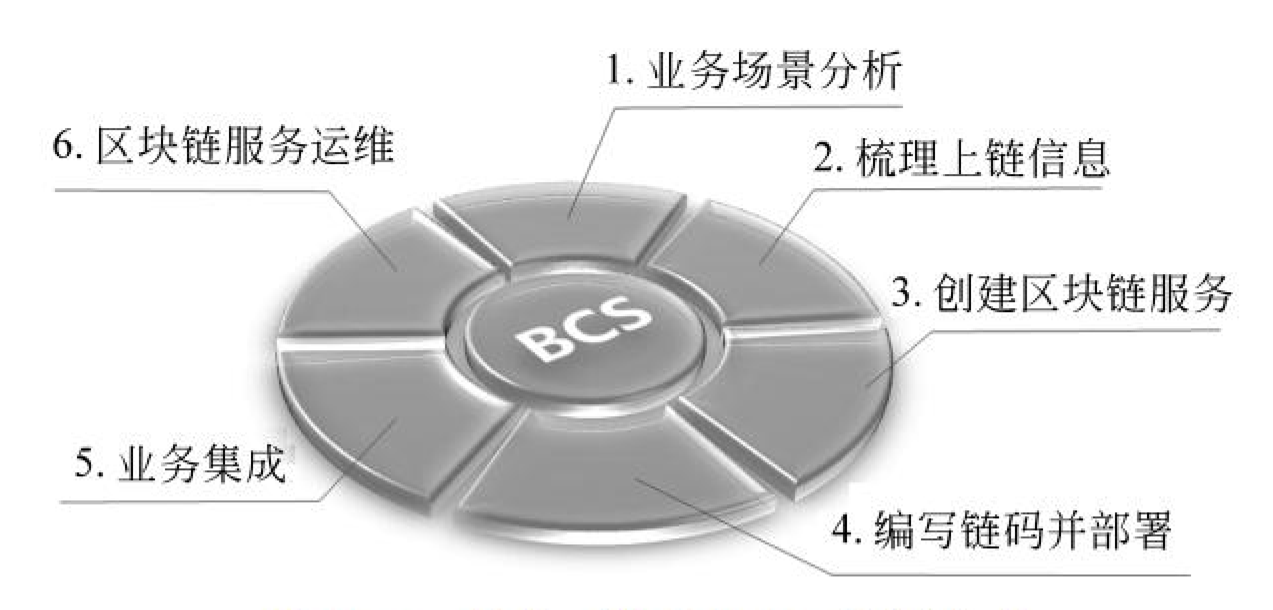


图 13.3 华为云构建企业区块链步骤

（1）业务场景分析：并非所有的应用都适合区块链，判定企业应用是否适合区块链应用至关重要。企业可以使用本书前面章节的区块链应用的判断准则进行判定。

（2）梳理上链信息：当判定应用为区块链应用后，也并非所有的数据都适合上链，企业还需要根据数据的业务特点和技术特性对上链数据进行选择和建模。

（3）创建区块链服务：华为云 BCS 服务提供一键式的购买，帮助用户屏蔽掉存储、网络、计算等相关资源的购买，系统自动完成大部分区块链底层平台所需配置。整体配置购买流程可以在 10 分钟以内完成（包括计算、资源和存储资源的创建时间）。

（4）编写链码并部署：链代码作为企业业务和区块链存储的纽带逻辑，是企业应用区块链化的结晶，在整个区块链应用开发过程中起着举足轻重的作用。华为云考虑到这一点，对这一环节提供了辅助增强，企业用户可以在线完成链代码的开发、部署与实例化，完成智能合约部分。

（5）业务集成：业务系统通过集成 SDK、调用 RESTful 或者 JDBC 的方式操作区块链，业务改动量小，简洁高效。

（6）区块链服务运维：通过对接华为云 AOM/APM，完成区块链实例、区块链应用的实时监控，提供日志、告警、性能指标的全方位监控，给业务的灵活变更提供依据。

下面将以一个完整的区块链应用为例，带领读者使用上述简单六步创建区块链应用，体验华为云区块链开发的极速之旅。

1. 业务场景分析

Marbles 是一个简单的资产转移示例业务，旨在帮助客户了解链码的基础知识以及如何使用华为 BCS 服务开发应用程序，帮助快速上手并体验华为云区块链服务。

图 13.4 是 Marbles 应用成品的界面演示，应用支持多个账户，每个账户可以创建自己的资产——弹珠，每个弹珠的规格都是随机并且独特的（有各自的颜色、大小），因此每一个弹珠都是“唯一”的。弹珠创建出来即为创建者所有，成为其资产。资产可以在用户之间互相转移，资产转移的动作称为交易。下面，我们先用前一章的区块链应用判断准则来分析一下该应用是否为区块链应用。

- 是否存储状态

Marbles 应用需要保存各种状态，包括用户的信息、弹珠的规格还有弹珠的归属权等，由

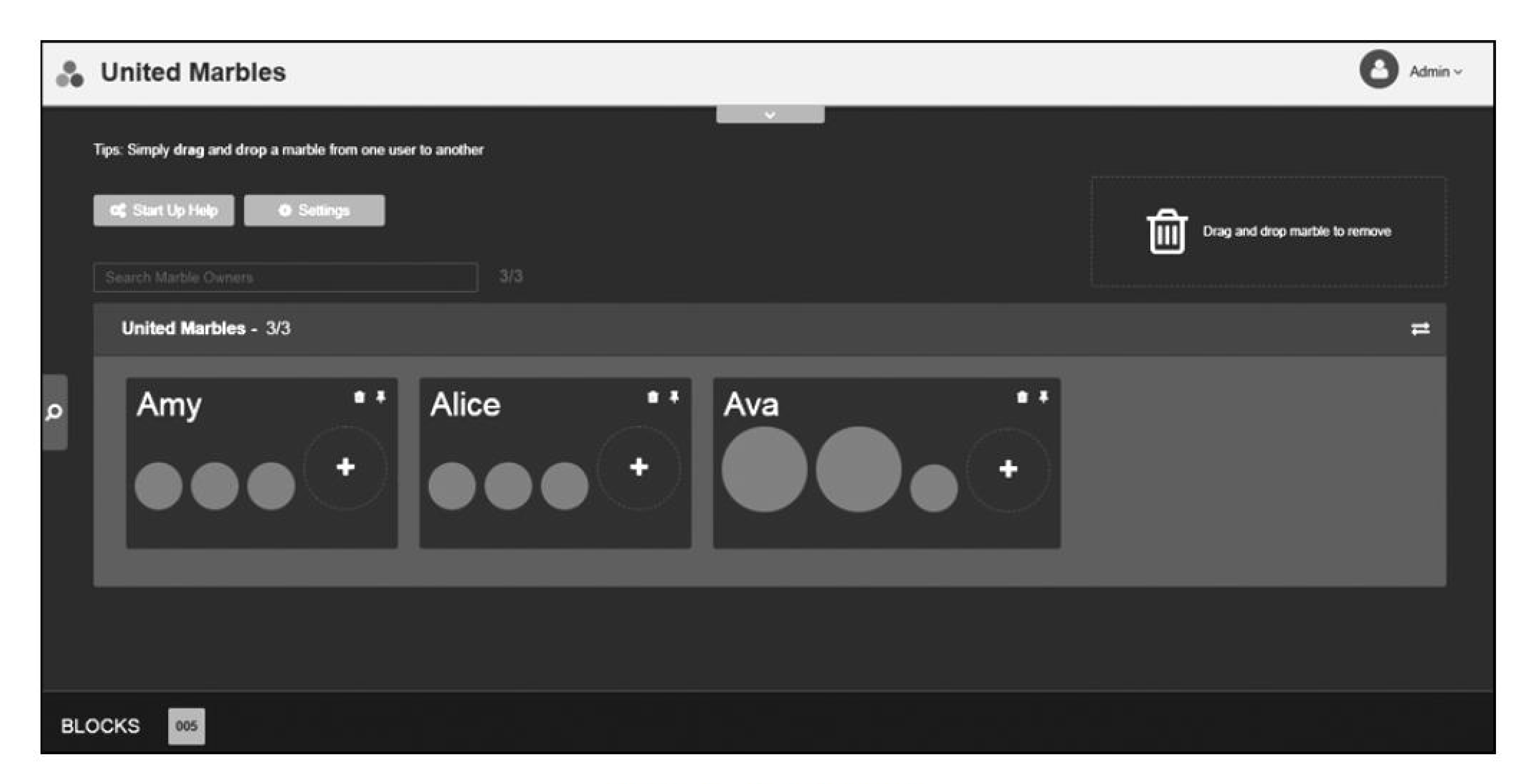


图 13.4 Marbles 界面

于弹珠可以转移所属权,转移的交易也需要进行记录,弹珠交易不能被任何一方随意更改,并且这些交易要保证安全,账户 A 只能转账户 A 的弹珠资产,这些状态数据的保持正是区块链所能提供的。

- 是否多方协作写入

弹珠资产转移是可以发生在任何两个账户之间的,并且交易的结果和用户的最终资产信息是需要向其他用户同步的,因此也符合区块链的多方协作写入的准则。

- 多方是否互信

显然,弹珠资产的所有权账户之间并不存在完全互信的关系,因此区块链所带来的信任是应用必不可少的。

- TTP 是否能完美解决

为弹珠资产构建一个可信任的第三方消耗巨大,而且很难找到一个让所有人都绝对信任的公信机构,即便能够找到,这种公信机构提供公信力的成本也是非常昂贵的,因此对于 Marbles 应用来说,使用区块链来代替中介机构是不二之选。

- 是否限制参与

我们并不希望任何能够接入互联网的人都能使用 Marbles 应用,因此使用联盟链建立一个准入门槛是必需的。

综上所述,我们判定 Marbles 应用是一个区块链应用,那么接下来我们就要看看都有哪些数据需要上链。

2. 梳理上链信息

在 Marbles Demo 中,我们的业务可以梳理为以下三条:

- 账户信息的创建,包括账户的增删改查

- 弹珠资产的创建,包括弹珠的增加与删除
- 弹珠资产的转移,资产转移发生在任意两个用户之间

由上所述,我们利用传统的软件分析能力不难分解出其中的名词:账户、弹珠资产。这两个实体将作为我们链上数据结构的实体模型。另外,我们还需要在弹珠模型上记录弹珠的所有权,即弹珠与账户的关系,因此我们得出了如下的数据模型,如表 13.2、表 13.3 所示,模型的数据都将以键值对的形式存储于区块链上。

表 13.2 弹珠实体数据模型表

Key	Value
ID	作为 Key 值使用,每一个 Marbles 资产的唯一标识
Color	资产的第一个属性,颜色
Size	资产的第二个属性,大小
Owner	资产的当前归属(至少包含账户的 ID)

表 13.3 账户实体数据模型表

Key	Value
ID	账户的唯一标示
Username	账户名称
Company	账户所属公司信息

然需要注意的是,我们此处给出的示例应用比较简单,大部分信息都存储在区块链上,然而实际的应用可能会非常复杂,数据量也将十分庞大,因此需分析具体业务来确定数据是否希望得到区块链的方便共享、安全写入和不可篡改等特性,只将必要的数据记录于区块链上,对于成本的控制和性能的保证是很关键的。

3. 购买区块链服务

在开发区块链应用之前,我们需要确保有一个真正的区块链平台可以供我们进行测试,以及将来作为实际的生产运行平台,从头搭建区块链平台是低效并且高风险的,选择华为云区块链服务可以为企业节省不少前期投入成本,以及后期维护成本,甚至降低对区块链使用的学习曲线。具体购买步骤如下:

(1) 注册华为云账号:用户可以登录华为云官网 https://www.huaweicloud.com,进行注册并实名认证。进入 BCS 控制台:华为云 BCS 服务可以在首页的产品菜单中找到,位于“企业应用”子栏目中,点击进入区块链服务,或直接访问 https://www.huaweicloud.com/product/bcs.html,如图 13.5 所示。

(2) 点击“立即体验”进入区块链服务控制台,如图 13.6。

(3) 点击控制台中区块链解决方案后侧的“开始部署”进入一站式部署区块链解决方案流程,按图 13.7 所示表格进行配置。

(4) 进入配置确认页面,对购买信息进行确认,如图 13.8,并点击提交进行购买。



图 13.5　华为 BCS 服务首页



图 13.6　区块链服务控制台

参数名	参数值	备注
计费模式	按需计费	选择包年模式价格更优惠
区块链服务名称	bcs-marbles	
版本类型	专业版	专业版支持联盟链
区块链类型	联盟链	
共识策略	FBFT	
安全机制	ECDSA	可选国密算法
版本信息	2.1.17	
链代码管理初始密码	Test@123	可自行设定
peer节点组织	org1:1节点	可以根据联盟创建多组织
共识节点数量	4	FBFT最少4个共识节点
存储方式	goleveldb	可选MySQL体验
通道配置	c12345：org1加入通道	
选择集群	不勾选	创建新集群
云主机个数	1	
云主机规格	2核4GB	
高可用	不启动	测试可以选择非高可用
云主机登录方式	密码	
root密码	Test@123	可自行设定

图 13.7 配置示例



图 13.8 配置确认页面

（5）购买过程会持续几分钟，主要用于虚机创建、CCE 容器集群创建、存储、EIP 的绑定，以及区块链网络的创建。创建完成后如图 13.9 所示提示创建成功。到这里，区块链实例就已经搭建完毕，剩下的为链码编写与业务对接，以及后续的运维工作。

现在我们已经有了一个底层的区块链基础设施，为了让其能够存储 Marbles 的业务数据，接下来我们需要向区块链服务编写和部署链代码，即我们的区块链业务逻辑。

4. 编写链码并部署

链代码也称智能合约，是控制区块链网络中相关方相互交互的业务逻辑。链代码将业务网络交易封装在代码中，最终在一个 Docker 容器内运行。目前华为云区块链服务暂时支持 Golang 语言编写代码。链代码即一个 Go 文件，创建好文件后进行函数开发等操作。

链码的开发主要是完成 Init 和 Invoke 两个函数：Init 函数用于初始化区块链的原始数据

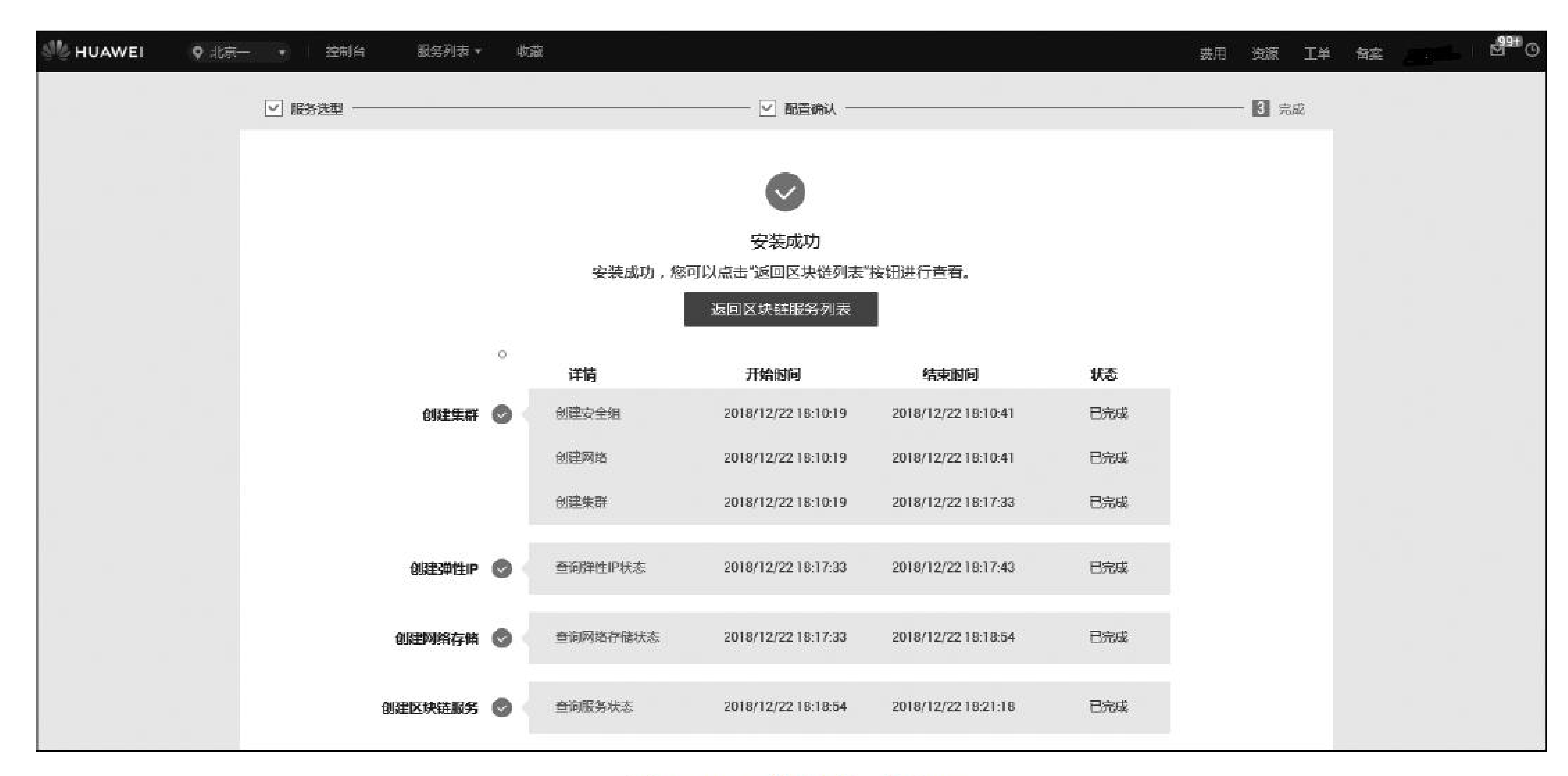


图 13.9　创建成功界面

结构，按需编写，也可以是一个空函数；Invoke 函数是主要的账本交互途径，可以完成追加账本、查询账本等操作，支持增加业务逻辑，完成复杂功能。我们不在这里赘述关于链码编写的详细规范，如果需要可以访问 Hyperledger 官网（https://hyperledger-fabric.readthedocs.io/en/latest/chaincode.html），或者咨询华为工程师进行了解（https://support.huaweicloud.com/devg-bcs/bcs_devg_0004.html）。

准备 Marbles Demo 所需链代码如下：完整的 Marbles Demo 链码可以在华为云官网获取，此处贴出的不完整的示例代码只为本书说明使用。

```
func init_marble(stub shim.ChaincodeStubInterface, args []string) (pb.Response){
    var err error
    fmt.Println("starting init_marble")

    id:=args[0]
    color:=strings.ToLower(args[1])
    owner_id:=args[3]
    authed_by_company:=args[4]
    size, err:=strconv.Atoi(args[2])
    if err !=nil {
        return shim.Error("3rd argument must be a numeric string")
    }

    //check if new owner exists
    owner, err:=get_owner(stub, owner_id)
    if err !=nil {
```

```
            fmt.Println("Failed to find owner - " + owner_id)
            return shim.Error(err.Error())
        }

        //check if marble id already exists
        marble, err:= get_marble(stub, id)
        if err == nil {
            fmt.Println("This marble already exists - " + id)
            fmt.Println(marble)
            return shim.Error("This marble already exists - " + id)   //all stop a marble by
            this id exists
        }

        //build the marble json string manually
        str:= `{
            "docType":"marble",
            "id": "` + id + `",
            "color": "` + color + `",
            "size": ` + strconv.Itoa(size) + `,
            "owner": {
                "id": "` + owner_id + `",
                "username": "` + owner.Username + `",
                "company": "` + owner.Company + `"
            }
        }`
        err = stub.PutState(id, []byte(str))     //store marble with id as key
        if err != nil {
            return shim.Error(err.Error())
        }

        fmt.Println("- end init_marble")
        return shim.Success(nil)
    }
```

前面的代码展示了创建弹珠资产的链代码,链码逻辑首先获取调用参数,进行了一系列业务逻辑合法性的检查,例如所述用户是否存在、弹珠 id 是否冲突等,然后生成新弹珠的信息并调用 stub. PutState 方法将弹珠信息保存到区块链。下面代码则是弹珠变更拥有者的链码:

```
    func set_owner(stub shim.ChaincodeStubInterface, args []string) pb.Response {
        var err error
        fmt.Println("starting set_owner")

        // input sanitation
```

```
    err = sanitize_arguments(args)
    if err != nil {
        return shim.Error(err.Error())
    }

    var marble_id = args[0]
    var new_owner_id = args[1]
    var authed_by_company = args[2]
    fmt.Println(marble_id + "->" + new_owner_id + " - |" + authed_by_company)

    // check if user already exists
    owner, err := get_owner(stub, new_owner_id)
    if err != nil {
        return shim.Error("This owner does not exist - " + new_owner_id)
    }

    // get marble's current state
    marbleAsBytes, err := stub.GetState(marble_id)
    if err != nil {
        return shim.Error("Failed to get marble")
    }
    res := Marble{}
    json.Unmarshal(marbleAsBytes, &res)   //un stringify it aka JSON.parse()

    // check authorizing company
    if res.Owner.Company != authed_by_company{
        return shim.Error("The company '" + authed_by_company + "' cannot authorize
    transfers '")
    }
    // transfer the marble
    res.Owner.Id = new_owner_id           //change the owner
    res.Owner.Username = owner.Username
    res.Owner.Company = owner.Company
    jsonAsBytes, _ := json.Marshal(res)   //convert to array of bytes
    err = stub.PutState(args[0], jsonAsBytes)   //rewrite the marble with id as key
    if err != nil {
        return shim.Error(err.Error())
    }

    fmt.Println("- end set owner")
    return shim.Success(nil)
}
```

与生成弹珠链码类似,首先获取参数信息,进行业务校验,然后最关键的部分则为更改弹

珠拥有者的信息以及将最新的弹珠信息存储到区块链上。

通常情况下，用户需要在线下搭建链码编写环境，自行编写与业务相关的区块链代码，包括准备相应语言的编辑器 IDE，创建区块链项目，引入和配置区块链 SDK 等，相当烦琐。华为云为了简化这一过程，提供用户线上的一键式体验，专门开发了适合编辑和调试区块链代码的线上编辑器，其特性如下：

- 语法高亮和自动补全提示

华为云链码在线编辑器暂时只支持 Golang 语言，对于 Golang 的语法关键字有高亮显示。类似大多数主 IDE，在用户输入关键词或变量前几个字母时会弹出联想列表，并且在变量或结构体后敲入“.”时会自动弹出该变量或结构体所有的方法，如图 13.10 所示，以节省编程者的时间。

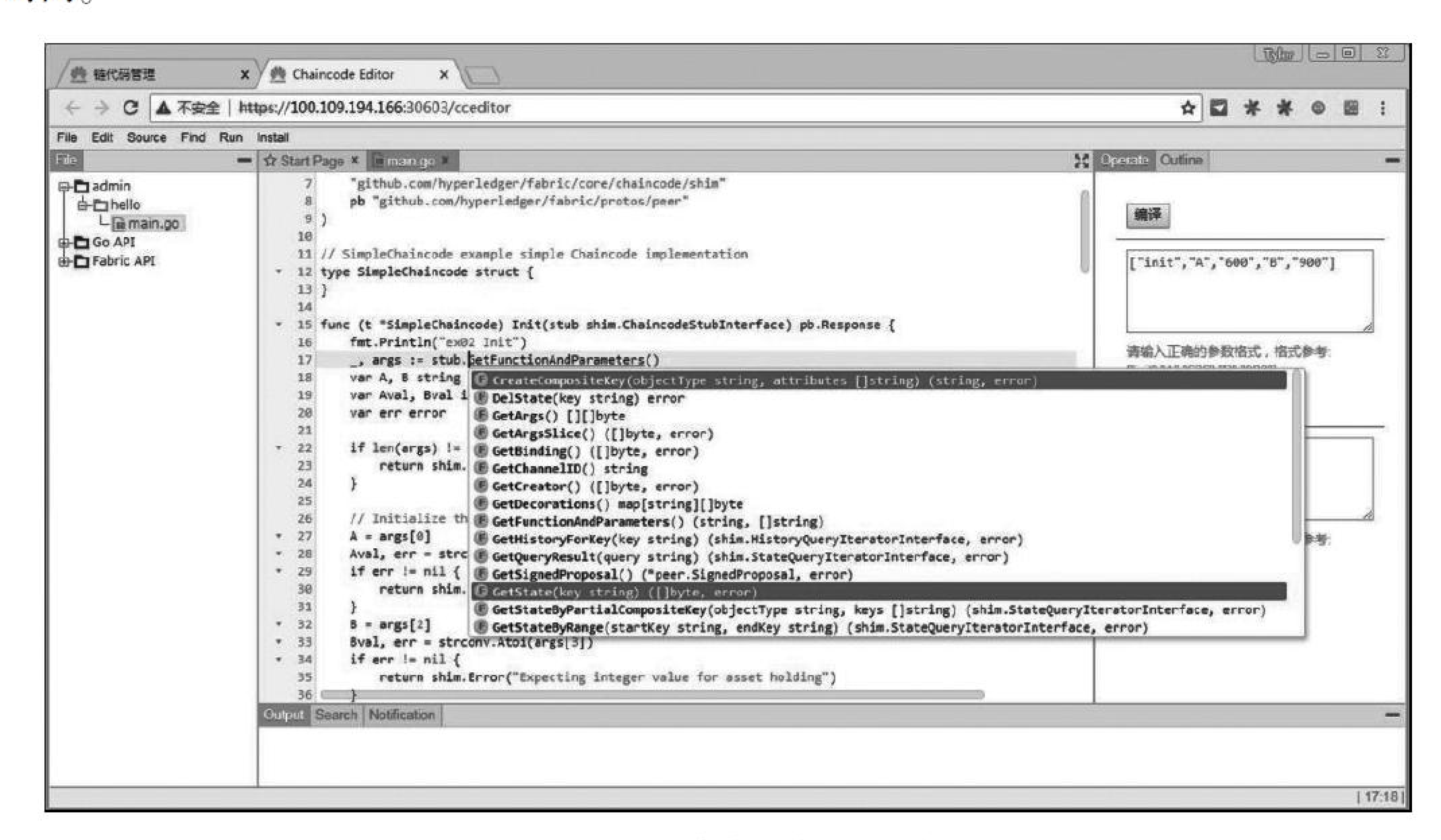


图 13.10　方法高亮和自动补全提示

- 查找方法声明

大多数程序员不喜欢在线编辑器的原因是因为在线编辑器有局限性，对于浏览阅读代码时查找方法或类型的声明和定义支持得不是很好。华为区块链编辑器可以让用户像使用本地 IDE 一样阅读代码，很方便地查找方法和类型的声明，如图 13.11 所示。

- 链码在线编译和语法错误提示

语法错误提示是任何一款 IDE 必不可缺的，很多轻量的编辑器只有语法检查，缺失的是编译部分。华为的在线链码编辑器可以实现编辑中自动保存和自动编译，使用户可更及时准确地发现链码编写错误，及时更正，如图 13.12 所示。

- 模拟链码初始化和调用

图 13.11　查找方法声明

图 13.12　链码在线编译和语法错误提示

模拟链码初始化和调用是普通编程语言 IDE 所不具备的，目前市面上几乎所有的 IDE 都只是针对某一编程语言进行支持，很少有对区块链链码编辑的特殊支持。使用华为云在线链码编辑器不但可以进行链码编译，更重要的是可以模拟链码初始化和调用，方便用户更早期地发现链代码中的问题，如图 13.13 所示。

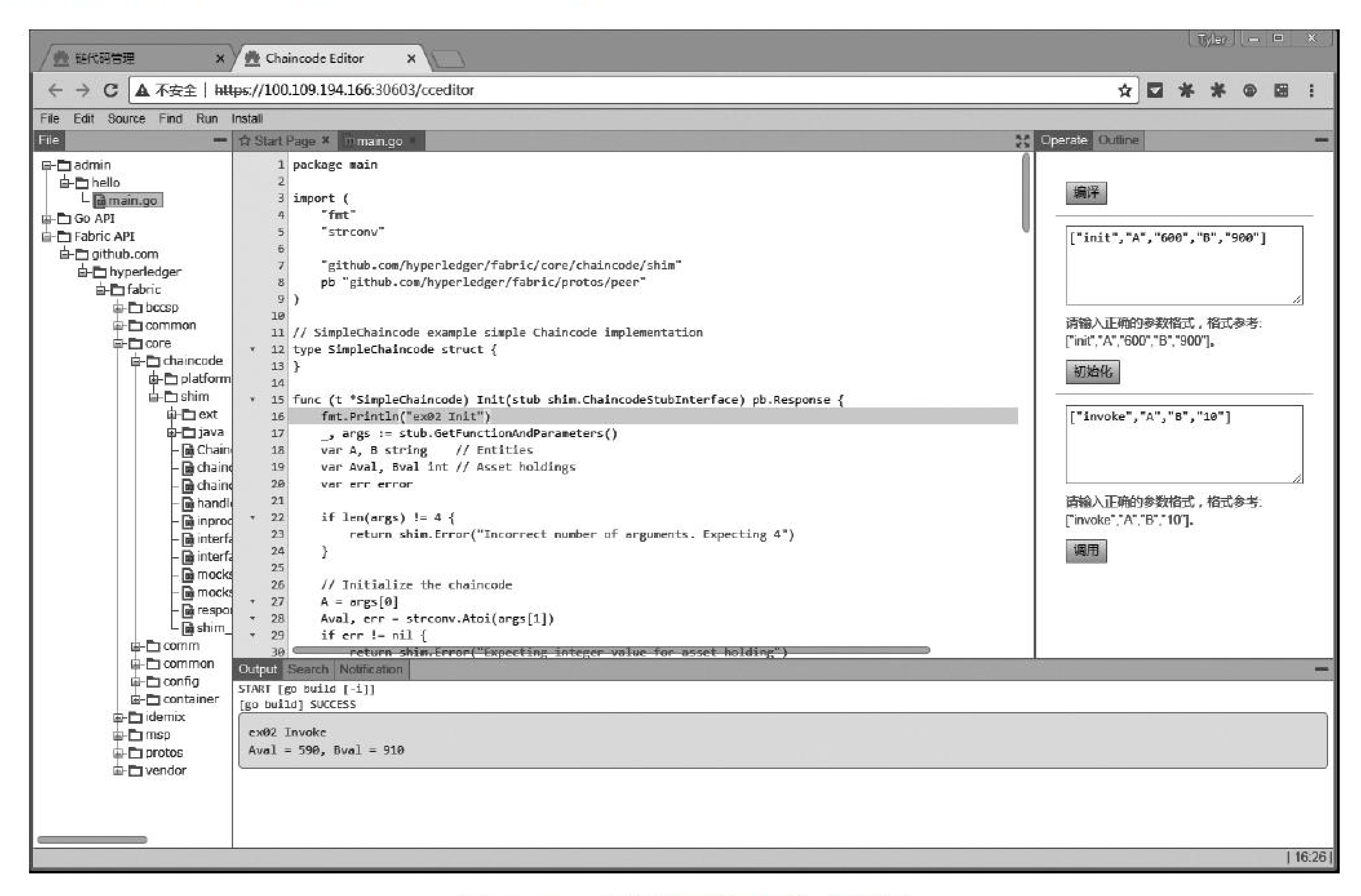


图 13.13　模拟链码初始化和调用

• 华为云区块链服务是基于 Hyperledger Fabric 开发，链代码编写完成后还要经过安装和实例化的步骤才能够供用户进行调用。华为云同样提供了非常便捷的链代码安装和实例化过程，如图 13.14 和图 13.15 所示，只要给出足够的信息，这些步骤都可以在线完成。

至此，Marbles 应用中区块链的部分已经开发和部署完毕，但仅有区块链是没有办法让最终用户来使用的，区块链的最终目的是服务于业务。接下来我们要将 Marbles 应用和刚刚构建的区块链服务对接，由应用触发业务数据在区块链上的存储和读取，才能发挥区块链的作用。

（5）业务系统集成

业务系统集成即对区块链服务与区块链应用进行集成对接，集成的速度和质量直接关系到应用开发人员的开发效率以及应用最终用户的体验，所以这一步是至关重要的。如图 13.16，由 Marbles 应用程序发起对资产转移链码的调用，试图将 user1 的弹珠资产 marble1 转移给用户 user2，调用触发链码逻辑先进行合法性校验，最终将弹珠资产 marble1 的所有者属性 user2 写到区块链上，完成资产的转移。

安装链代码

* 链代码名称　marbles

* 链代码版本　1.0

账本数据存储方式　文件数据库(goleveldb)

组织&Peer节点　peer-1 ×

链代码语言　golang

链代码文件　添加文件　fabbankid.zip

链代码描述　请输入描述信息

0/500

安装　取消

图 13.14　安装链代码



图 13.15　链代码实例化

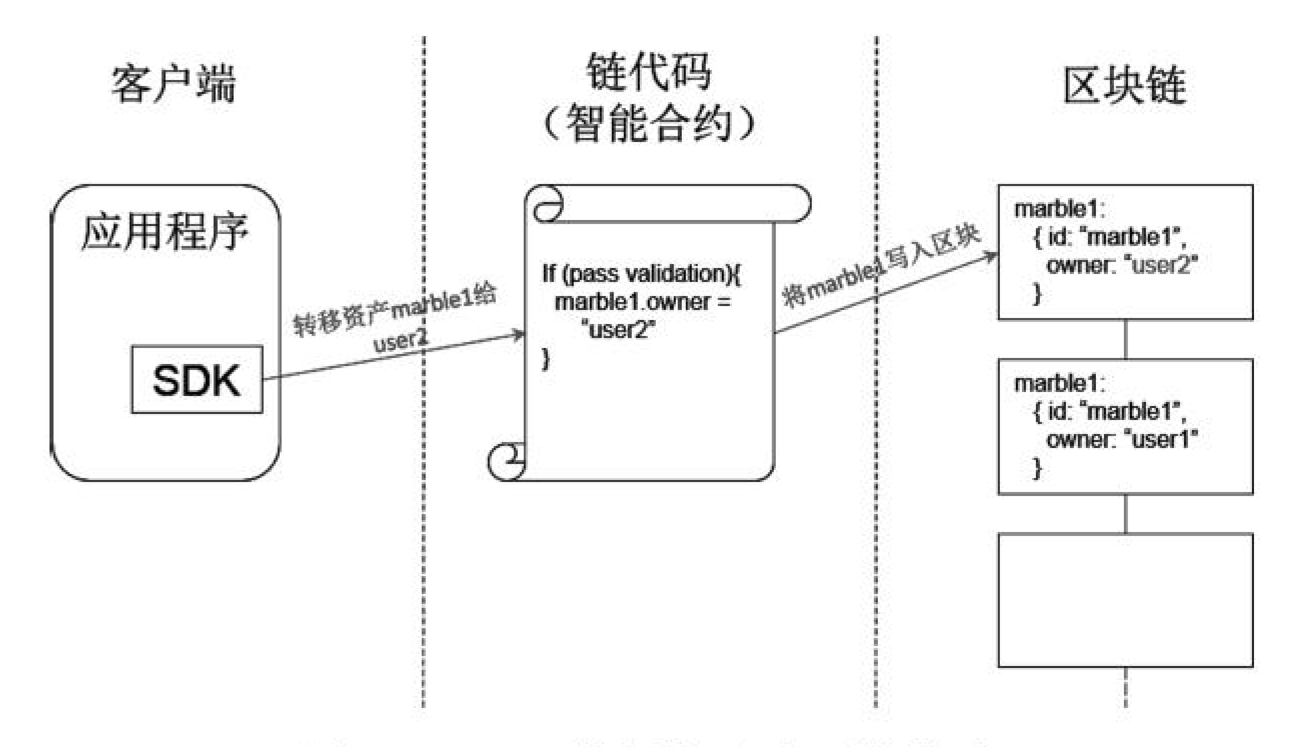


图 13.16　区块链与业务系统集成

那么在上述业务流程中，Marbles 应用程序具体需要如何跟区块链的链代码交互呢？图 13.17 阐述了交互的细节：

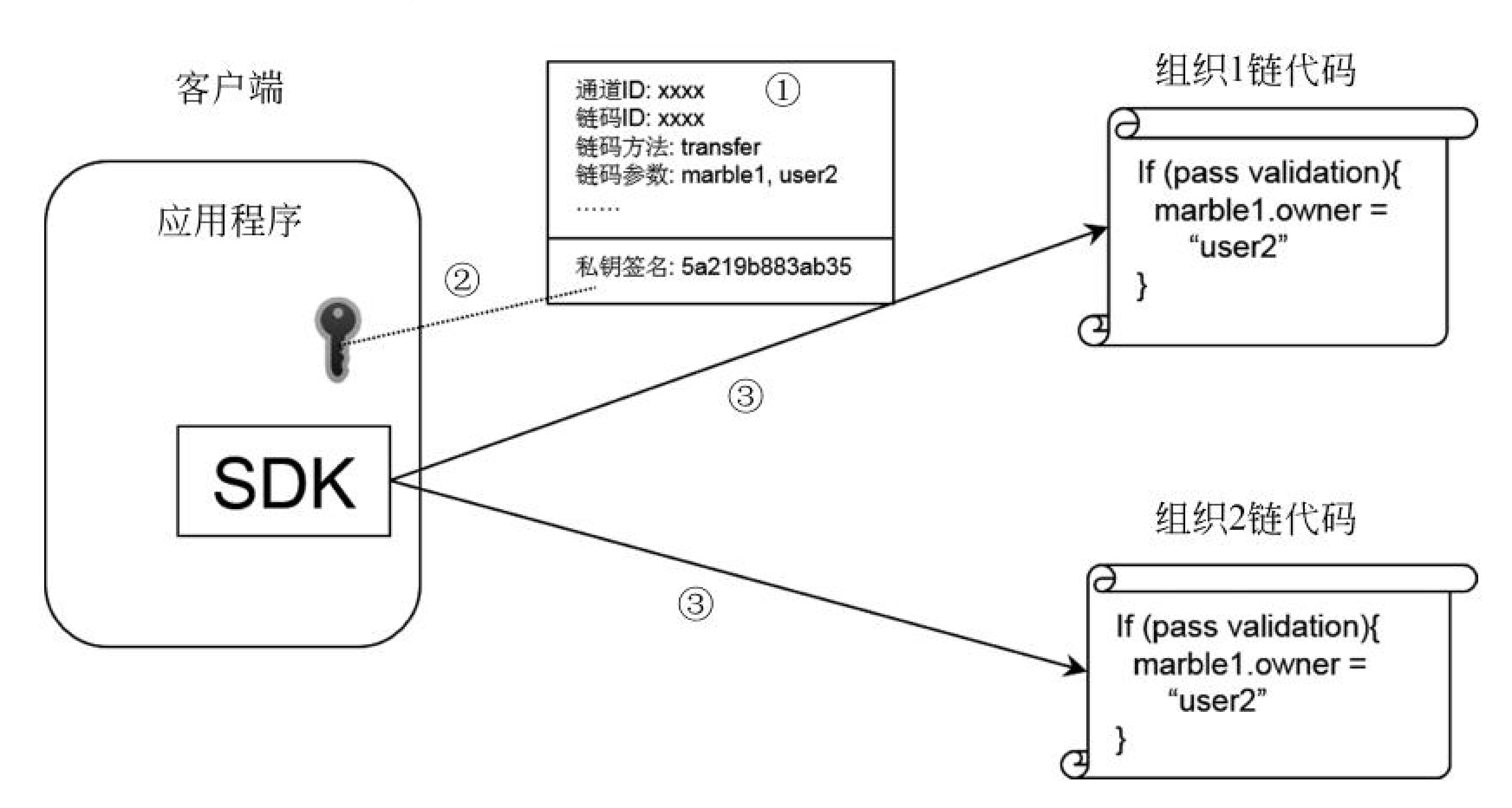


图 13.17　应用程序与区块链代码交互步骤

① 客户端将调用块链码所需要的信息进行打包，包括通道 ID、链码 ID、调用参数、调用者信息等。

② 客户端将步骤①打包好的二进制用调用者私钥进行签名，此签名除了拥有私钥的用户外，其他人无法伪造。

③ 最后客户端将前两步产生的二进制及签名分别发到需要背书的区块链节点进行背书，背书的过程即为链码调用的过程。然后，客户端将返回的背书信息汇总发送到区块链上进行写入。

由此我们可以看到，应用程序和链码的交互过程还是比较复杂的，这个过程不应该让应用开发者自己来实现，因此就有了支持各种语言的客户端 SDK 版本，例如 Golang、Node. js 等。但即便如此，使用客户端 SDK 的成本还是很高，因此华为云提供了两种调用方式：一种是刚

才提到的使用语言相关的客户端 SDK 进行调用；另外一种为创新的 RESTful 调用方式，如图 13.18 所示。

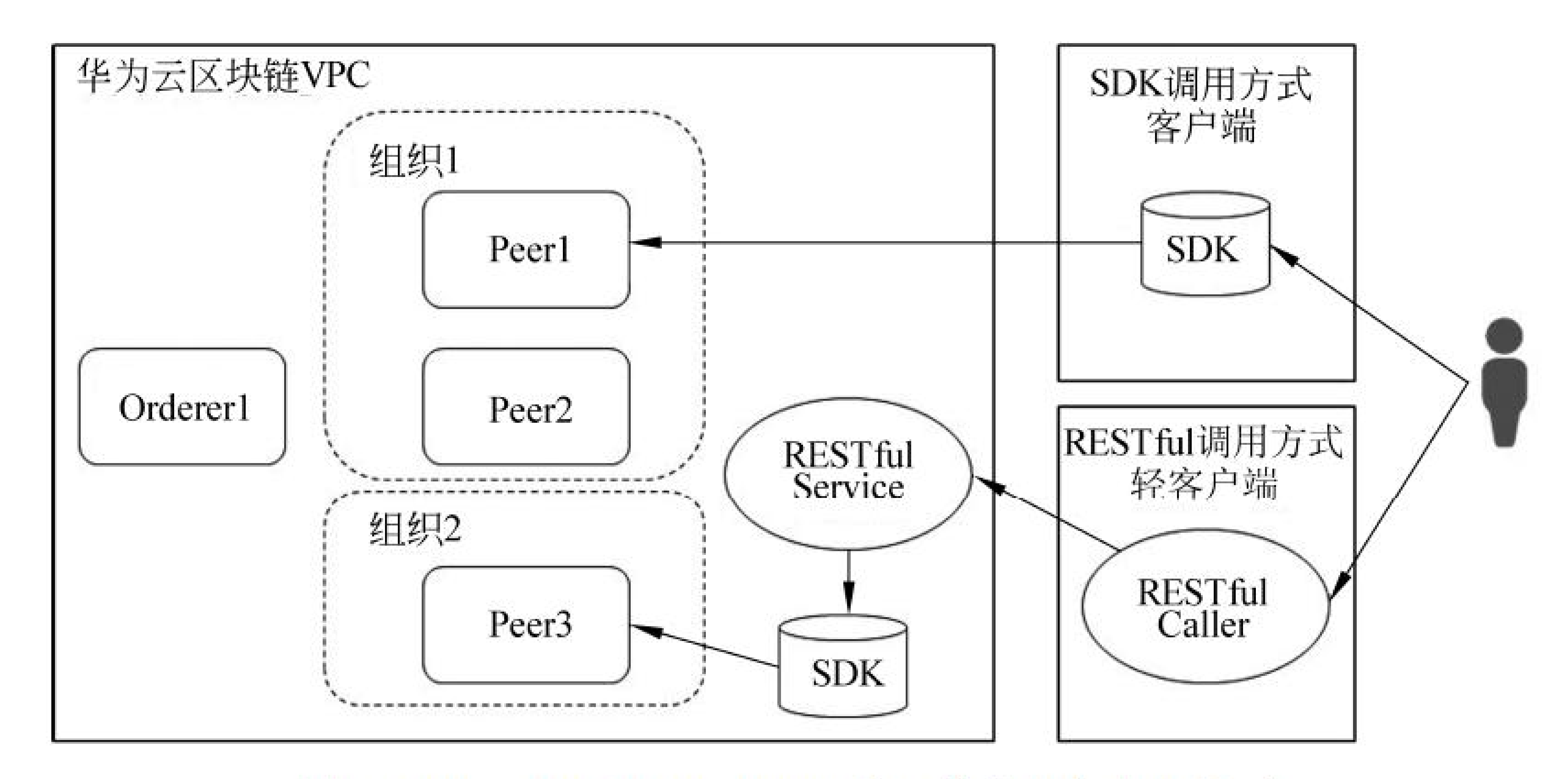


图 13.18　SDK 和 RESTful 两种区块链服务调用方式

接下来分别向读者详细介绍这两种调用方式。

- SDK 对接方式：

开发业务应用时需要根据所使用的开发语言种类确定下载的 SDK，如 Marbles 应用使用 Node. js 作为开发语言，BCS 服务提供了相应的 SDK 配置文件下载，见图 13.19 和图 13.20 所示。

图 13.19　下载 SDK 配置

SDK 配置文件是为了让区块链 SDK 调用程序了解已经完成部署的区块链服务的架构、peer 和 orderer 的地址以及各种证书的位置等，这些信息都是使用 SDK 所必需的。SDK 获取之后，就可以使用 SDK 开发区块链调用代码了。本例中创建弹珠的方法由 Node. js-SDK 实现，代码示例片段如下所示：

```
marbles_chaincode.create_a_marble = function (options, cb) {
```

配置SDK文件

* 链代码名称 marbles

* 链代码版本 1.0

* 证书存放根路径 /opt/gopath

通道名称 test

组织&Peer节点 peer-193a9195564941cb194ec...

下载 取消

图 13.20 SDK 配置信息

```
console.log('');
logger.info('Creating a marble...');

var opts = {
    peer_urls: g_options.peer_urls,
    peer_tls_opts: g_options.peer_tls_opts,
    channel_id: g_options.channel_id,
    chaincode_id: g_options.chaincode_id,
    chaincode_version: g_options.chaincode_version,
    event_urls: g_options.event_urls,
    endorsed_hook: options.endorsed_hook,
    ordered_hook: options.ordered_hook,
    cc_function: 'init_marble',
    cc_args: [
        'm' + leftPad(Date.now() + randStr(5), 19),
        options.args.color,
        options.args.size,
        options.args.owner_id,
        options.args.auth_company
    ],
};
fcw.invoke_chaincode(enrollObj, opts, function (err, resp) {
      if (cb) {
          if (! resp) resp = {};
```

```
                resp.id = opts.cc_args[0];//pass marble id back
                cb(err, resp);
            }
        });
};
```

从代码片段我们可以看到,使用 SDK 进行链码调用分为两步: 第一步构造调用参数,声明要调用的区块链通道和链码 id 等,然后是链码的业务参数,本例中根据已经部署好的 Marbles 链码的要求传入弹珠颜色、大小等参数即可;第二步是真正发起链码调用的 SDK 方法,只有一行代码,调用 fcs. invoke_chaincode 即可实现链码调用,剩余的代码为错误处理通用代码。由此可见,SDK 的使用还是很简单的。接下来的变更弹珠资产所有者的代码与刚才的创建弹珠代码类似,如下所示:

```
marbles_chaincode.set_marble_owner = function (options, cb) {
    console.log('');
    logger.info('Setting marble owner...');

    var opts = {
        peer_urls: g_options.peer_urls,
        peer_tls_opts: g_options.peer_tls_opts,
        channel_id: g_options.channel_id,
        chaincode_id: g_options.chaincode_id,
        chaincode_version: g_options.chaincode_version,
        event_urls: g_options.event_urls,
        endorsed_hook: options.endorsed_hook,
        ordered_hook: options.ordered_hook,
        cc_function: 'set_owner',
        cc_args: [
            options.args.marble_id,
            options.args.owner_id,
            options.args.auth_company
        ],
    };
    fcw.invoke_chaincode(enrollObj, opts, cb);
};
```

Node. js SDK 也是先构造参数,传入弹珠 ID 和拥有者 ID,然后使用 fcw. invoke_chaincode 发起实际的链码调用,非常简单。由于开发语言众多,其他 SDK 的使用方法不在此赘述,请自行查阅相关文档。在此只探讨一下 SDK 开发方式的优缺点。

优点: 基于原生 Fabric SDK, 没有其他环节,调用响应速度较快。

缺点:

- 配置文件书写复杂

虽然华为云已经提供了 SDK 配置文件下载功能，对于首次使用 SDK 的开发人员来说成本仍然很高。

- SDK 与语言相关，并且学习成本略高

虽然很多语言都提供了 Fabric SDK，SDK 调用起来也算是简洁，但使用起来仍然有一定学习成本，并且不同语言的类库名称、方法名称调用方式都各不相同，切换不同语言时的学习成本成倍增加。

- SDK 过于厚重

应用程序在使用 SDK 的时候需要将 SDK 类库引入，虽然不用开发语言的 SDK 打包后大小各不相同，但对于一些薄客户端（比如手机应用）来说就显得十分厚重了。

- RESTful 对接方式：

华为云为了方便开发者使用区块链服务，在服务侧提供了 RESTful 的 API 以克服上述直接使用 SDK 方式的不足。要使用 RESTful 对接方式，只需在订购时选择启用 RESTful 接口即可，并且如果订购时候没有选择，后续也可单独进行安装，安装好 RESTful 接口的服务见图 13.21 中的 RESTAPI 组件。

^ bcs-zmm　正常　联盟链　专业版　测试策略(SOLO)　2018/11/27 15:26:...　链代码&区块管理　更多 ▾

组织名称	组织状态	组织类型	实例数(正常/总数)	操作
bcs-zmm-orderer	正常	共识	1/1	下载管理员证书
organization1	正常	节点	2/2	伸缩　下载管理员证书　更多 ▾
organization2	正常	节点	2/2	伸缩　下载管理员证书　更多 ▾
baas-restapi	正常	RESTAPI	1/1	伸缩
baas-agent	正常	代理	1/1	

图 13.21　订购了 RESTful 组件的区块链服务

一旦添加了 RESTful 服务，即可使用相关语言中的 RESTful 方式进行调用。因为华为云替用户管理着区块链的组织结构以及各种证书，所以天然具备了所需要的 SDK 的配置文件，不需要用户自己手动生成。在此先给出一个 RESTful 链码调用请求的 Header 和 Body 的示例供读者参考，如图 13.22 所示。

RESTful 已经作为一种最基本的远程调用形式在各大语言中都有非常良好的支持，在此就不做赘述了，比较特殊的地方是请求中 Header 的签名字段 x-bcs-signature-sign 和 Body 里面的 cert 证书字段。请读者不要着急，下面先给大家详细阐述华为区块链服务的 RESTful 接口的机制，了解了原理后这两个特殊字段的含义就会清楚了。

根据本节一开始在图 13.17 中所描述的应用程序与区块链代码交互步骤中，客户端所做的工作除了包装方法调用参数之外，最重要的一项工作就是进行签名，签名可以保证交易不会被其他人冒充。那么 RESTful 调用同样也存在这个问题，RESTful 是基于 HTTP 协议的，更为通用，因此在安全上我们更要做好充足的工作以保证其不可被冒充，图 13.23 阐述了华为

```
HEADER:
x-bcs-signature-sign:
1f8b08000000000000ff14cbb11503510c02b081d260c098bfff6279d74bb90a5ca7384e3cae9b5825af7cb076b65e039be41da8e8b1e38700d599fa4aee37d6c159a9
4355ada783dbb4d66e17e967db39cef36bcd0b5adc8be3e178698ef9070000ffff

BODY:

{
  "channelId": "mychannel",
  "chaincodeId": "marbles",
  "chaincodeVersion": "1.0",
  "userId": "User1",
  "orgId": "7258adda1803f4137eff4813e7aba323018200c5",
  "opmethod": "invoke",
  "args": "[\"set_marbles\",\"marble1\",\"User2\"]",
  "timestamp": "2018-10-31T17:28:16+08:00",
  "cert": "-----BEGIN CERTIFICATE-----
\nMIIDBzCCAq2gAwIBAgIQEXPZ1MsReamxVtVNnKwCCzAKBggqhkj0PQQDAjCCAQQx\nDjAMBgNVBAYTBUNISU5BMRAwDgYDVQQIEwdCRU1KSU5HMRAwMwUQYD14eH+jTTBLMA
4GA1Ud\nDwEB/wQEAwIHgDAMBgNVHRMBAf8EAjAAMCsGA1UdIwQkMCKAIFBXQ5TC4acFeT1T\nJuDZg62XkXCdnOfvbejSeKI2TXoIMAoGCCqGSM49BAMCA0gAMEUCIQCadHIK
10Mk\nYn0WZizyDZYR4rT2q0nzjFaiW+YfV5FBjAIgNalKUe3rIwXJvXORV4ZXurEua2Ag\nQmhcjRnVwPTjpTE=\n-----END CERTIFICATE-----\n"
}
```

图 13.22　RESTful 链码调用请求

RESTful 链码调用的机理。

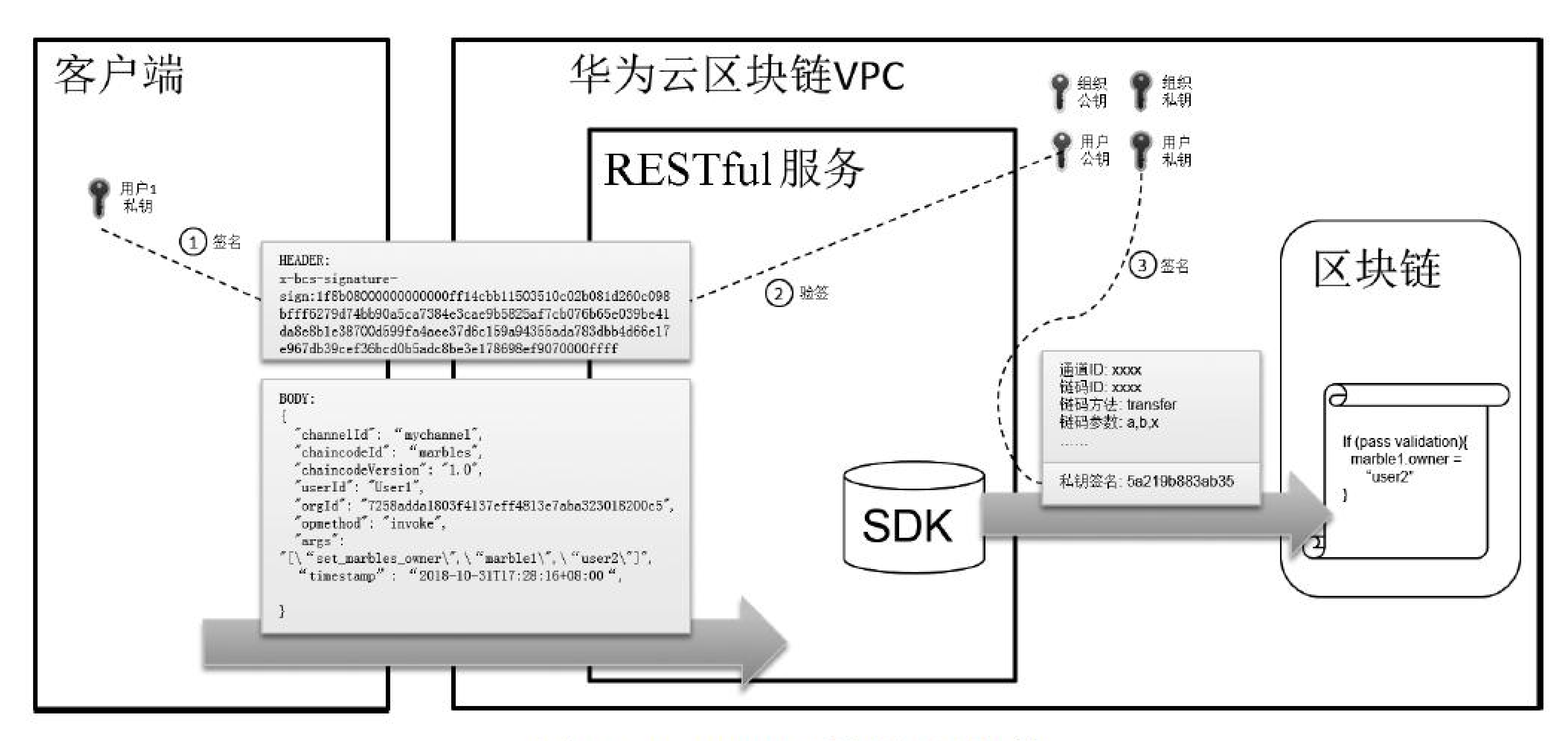


图 13.23　RESTful 链码调用机制

华为云利用开源区块链已有的 MSP 功能所提供的安全架构，使用和 SDK 类似的方式对交易进行保障。在客户端发起 RESTful 链码调用时，首先使用用户的私钥对整个 RESTful 方法体进行签名，如图中①所示。签名的结果放到 Header 的 x-bcs-signature-sign 字段中。RESTful 服务端接收到请求后，会使用用户的公钥对请求进行验签，如图中②所示。RESTful 服务内部封装了对开源 SDK 的调用，SDK 会重新包装链码调用信息，使用用户私钥对其进行

再次签名,如图中③所示,以此完成对链代码的调用。

另外还有一种更为复杂的场景。当用户自行管理证书的时候,我们的服务端是没有用户公私钥对的,此时用户用私钥签名之后,服务端无法进行验证,所以这种场景就要求用户将自己的公钥随着请求传到服务端,如图 13.24 所示:

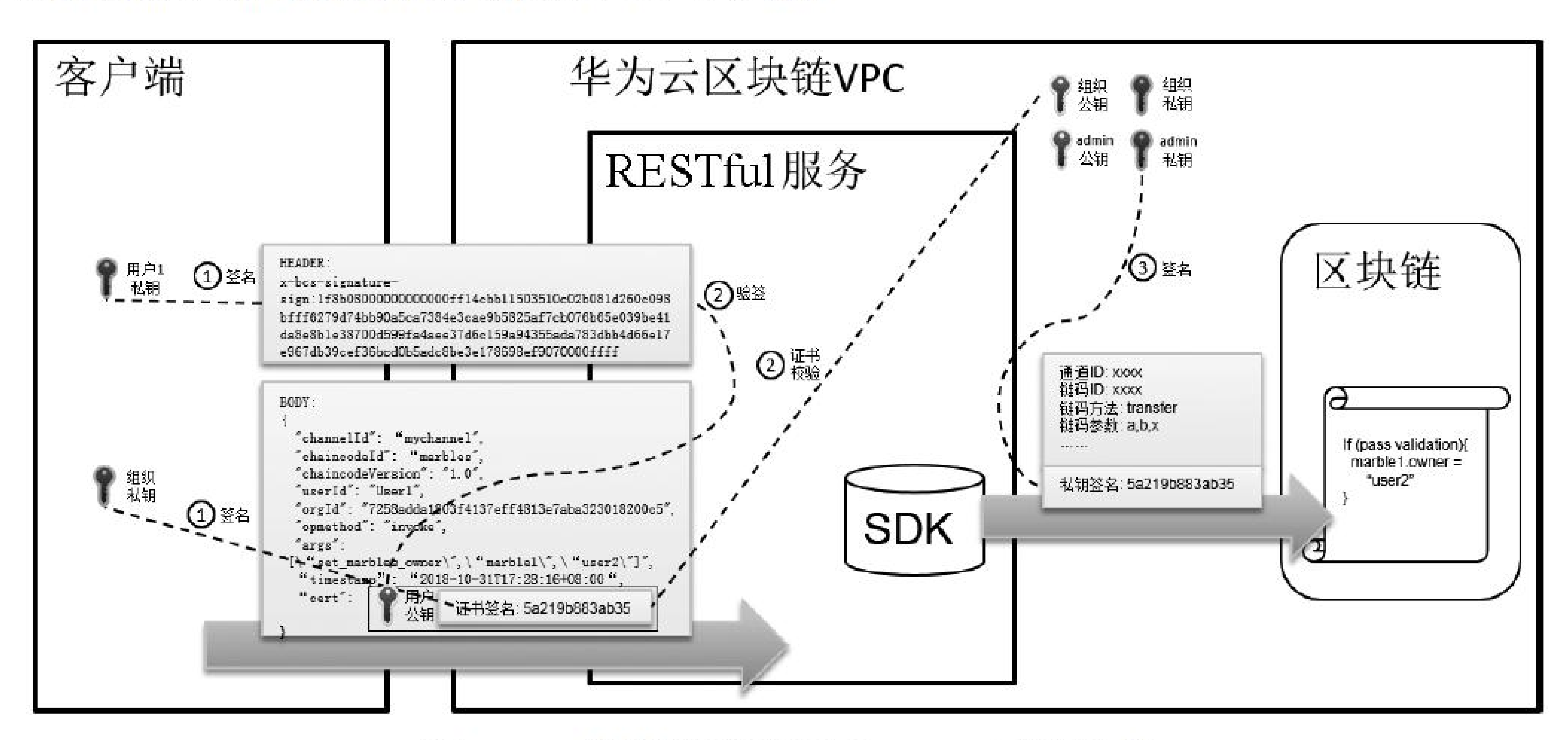


图 13.24 用户管理密钥对的 RESTful 调用过程

用户自己管理的证书也不可以随意生成,必须由组织的私钥签发才有效,因此在用户发起 RESTful 请求时,如图中①所示,要在请求体中放入证书,证书包含用户的公钥以及组织私钥的签名,然后再将整个请求体使用用户私钥进行签名,将签名结果放到 Header 的 x-bcs-signature-sign 字段。

请求到达服务端后,如图中②所示,服务端首先使用组织的公钥对上传的证书进行合法性校验,校验通过则说明用户上传的证书确实是组织签发,用户公钥合法有效,可以使用证书对 Header 中的签名进行校验。校验的过程以及后续步骤跟之前的场景相同,在此就不赘述了。

至此,相信读者已经对华为区块链服务的 RESTful 链码调用 API 机制有了深刻的了解,那么这种调用方法和普通的 SDK 方式相比有什么优势呢? 在此,我们进行简单的归纳如下:

- 使用简单方便,由华为云区块链服务封装 SDK 的复杂性。
- 由于绝大多数语言都已经拥有很成熟的 RESTful 调用类库,调用 RESTful 基本没有学习成本。
- 不用引入 SDK 类库,适合更轻量的客户端。

由上可以看出,RESTful 使用起来更加方便,但我们的 Marbles 示例为了展示更复杂的调用方式选择了 SDK 对接,至此,我们的 Marbles 应用已经可以正常运行。

另外需要注意的是,上述两种对接方式的优缺点只代表了普通的场景,真实场景如何选择还需要结合实际情况进行分析。例如用户购买了足够的带宽,RESTful 调用开销和延时已经不是瓶颈,并且 RESTful 服务内部对 SDK 也进行了缓存,此时在大规模调用的情况下使用

RESTful 对接方式的性能可能占优。

（6）区块链服务运维

我们知道，任何 IT 系统都离不开运维，区块链应用也一样，运维的内容包括对软件服务的管理、对系统底层资源的监控以及对应用日志的收集等。下面就针对一些华为区块链服务运维中的典型场景进行介绍。

- 服务扩容

华为区块链服务基于开源的 Hyperledger Fabric，每个组织有一些数量的节点（Peer）用来对交易做背书，当交易量增大时，为了保证背书效率，就需要对节点数量进行扩容。华为云提供了以下简单易行的扩容方式。

首先，进入区块链服务控制台，选择“服务管理”，点开 marbles 左侧的下拉箭头，见图 13.25 所示：



图 13.25　服务列表

然后点击 org1 栏最后的“伸缩”，调整实例个数为 3，点击确认，提示节点扩容成功，见图 13.26 所示。



图 13.26　节点伸缩

刷新页面，可以看到 org1 的实例个数已经扩展到 3 个，见图 13.27 所示。

- 资源监控

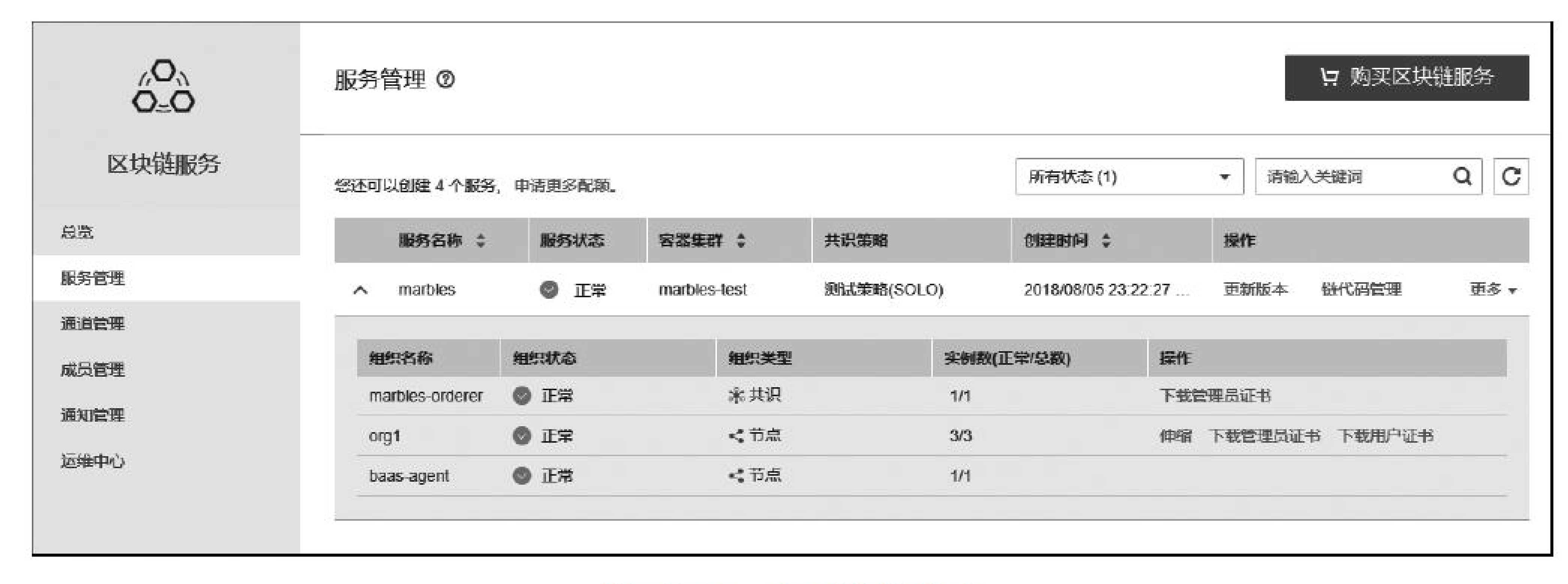


图 13.27　节点伸缩成功

我们需要一个整体的可视化监控界面，可以查看节点（虚机）、peer、orderer 性能指标：进入区块链服务控制台，点击“运维中心”，跳转到应用运维管理控制台，如图 13.28 所示。



图 13.28　运维管理控制台

选择左侧的“主机监控”，可以看到我们的虚机节点的性能指标，如图 13.29 所示。

选择左侧“容器监控”→“工作负载”，可以看到所有应用的性能指标，如图 13.30 所示，包括虚机上的 orderer、peer、系统运行所需的代理等几个服务，我们重点关注 peer 和 orderer 两个。

点击 Peer，跳转到应用监控，可以看到 peer 应用整体和每个 peer 实例的性能指标，如图 13.31 所示。

再点击某一个 peer 实例，即可看到实例详细的性能指标，点击浏览器的返回，或者左上角的返回箭头，可以返回上一级。

全部 | 正常 | 异常 | 已删除　集群：全部　请输入主机名称、别名、　更多

主机名称	主机IP	主机状...	所属集...	CPU使用率(%)	物理内存使用率(...	虚拟内存使用率(...	磁盘使用率(%)	操作
cce-demo15...	192.168.189.210	异常	cce-dem...	--	--	--	--	操作
cluster-bcs-2...	192.168.0.228	正常	cluster-bc...	11.2	27.1	41.9	1.883	操作

图 13.29　主机性能指标

全部 | 正常 | 异常 | 已删除　集群：全部　请输入负载名称　更多

负载名称	实例数(正常/全部)	状态	所属集群	CPU使用率(%)	物理内存使用率(%)
baas-agent	1/1	正常	cluster-bcs-2cdj	0.35	1.48
orderer-806b4a2d7296...	4/4	正常	cluster-bcs-2cdj	0	0.258
peer-da900c18bfa8a53...	1/1	正常	cluster-bcs-2cdj	0.4	0.997

图 13.30　区块链应用各组件性能指标

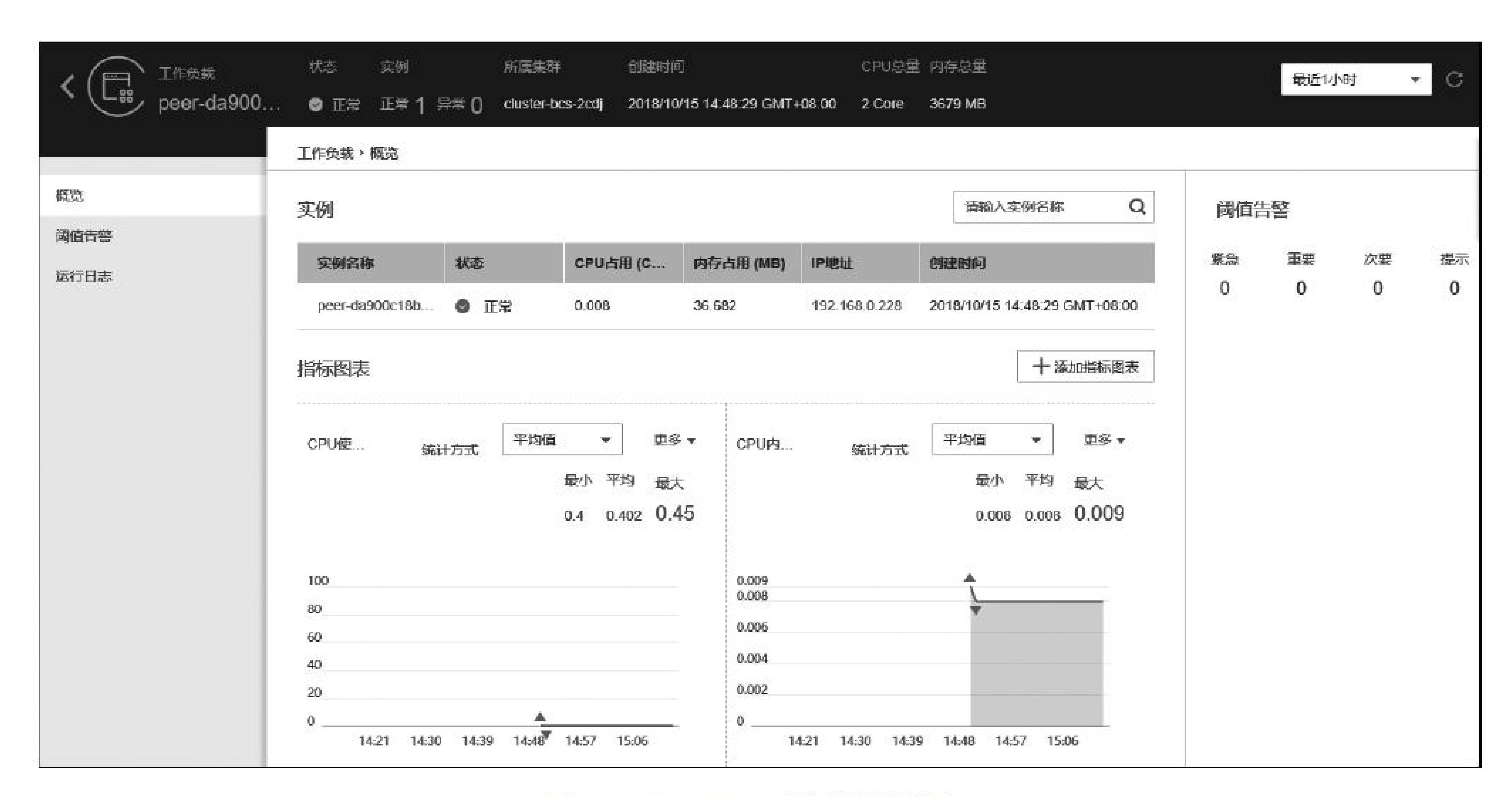


图 13.31　Peer 实例性能指标

- 主机扩容

虚机节点的扩容我们需要使用到云容器引擎(CCE)如图 13.32 所示。选择产品→计算→CCE 服务,点击立即使用,进入 CCE 控制台,在控制台,也可以看到集群、节点、容器的性能指标。

选择左侧的资源管理→集群管理,点击新增节点→购买节点,跳转到节点购买页面,全部可以选择默认,在登录上添加密码,点击立即购买,跳转到规格确认页面,点击提交,随后虚拟

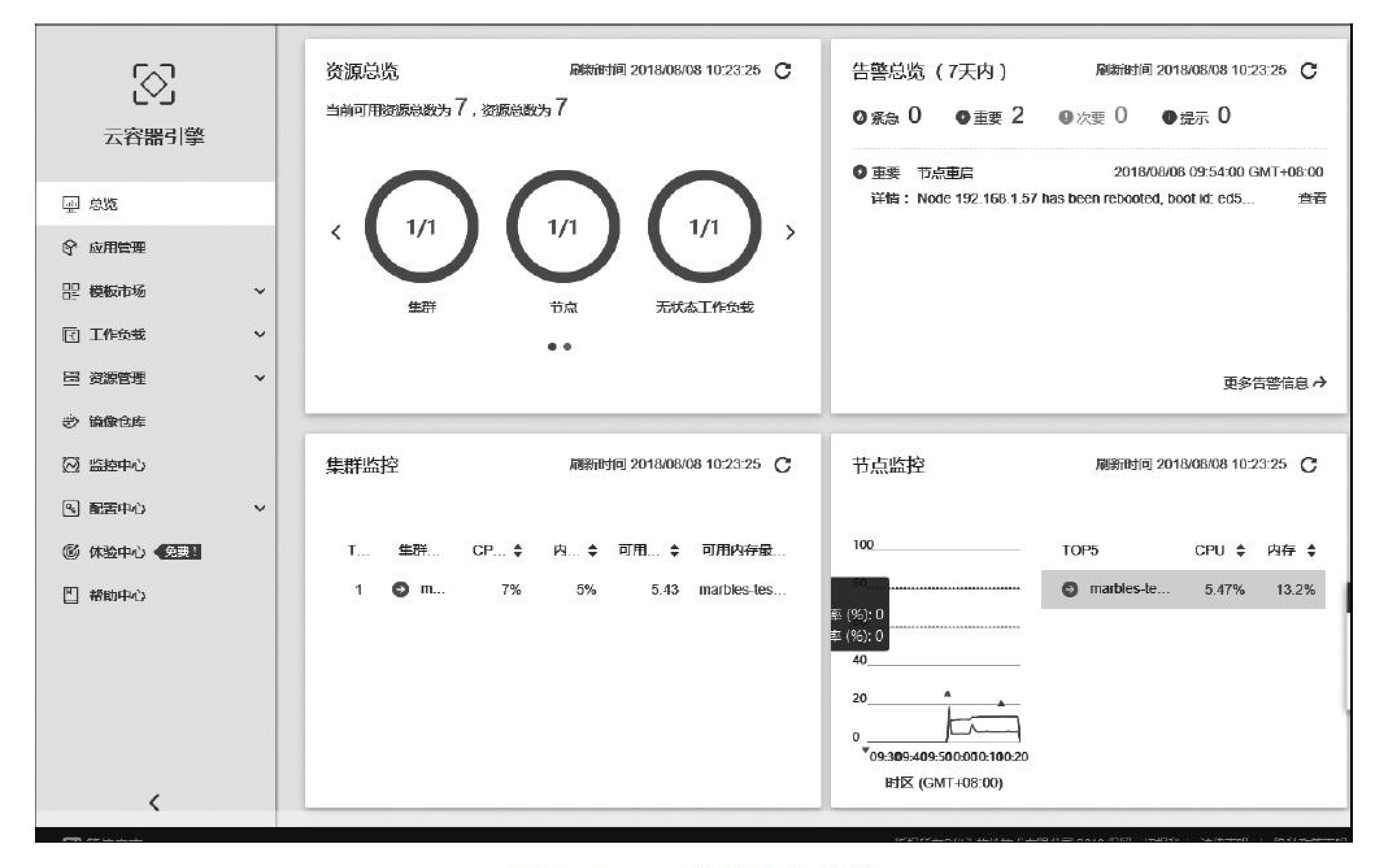


图 13.32　云容器引擎总览

机就开始创建。大约几分钟后，到 CCE 集群管理界面可以看到当前集群中已经有两个节点可以使用，如图 13.33 所示。



图 13.33　主机扩容成功

- 查看容器日志

华为云大部分服务都是容器化的，区块链服务也不例外。区块链的容器日志也可以同时

在 CCE 和运维中心看到,我们这里推荐在运维中心查看。进入区块链控制台,点击运维中心,进入应用监控页面(指标→应用→peer→选择一个 peer 实例),点击运行日志,即可看到容器运行的相关日志,如图 13.34 所示。

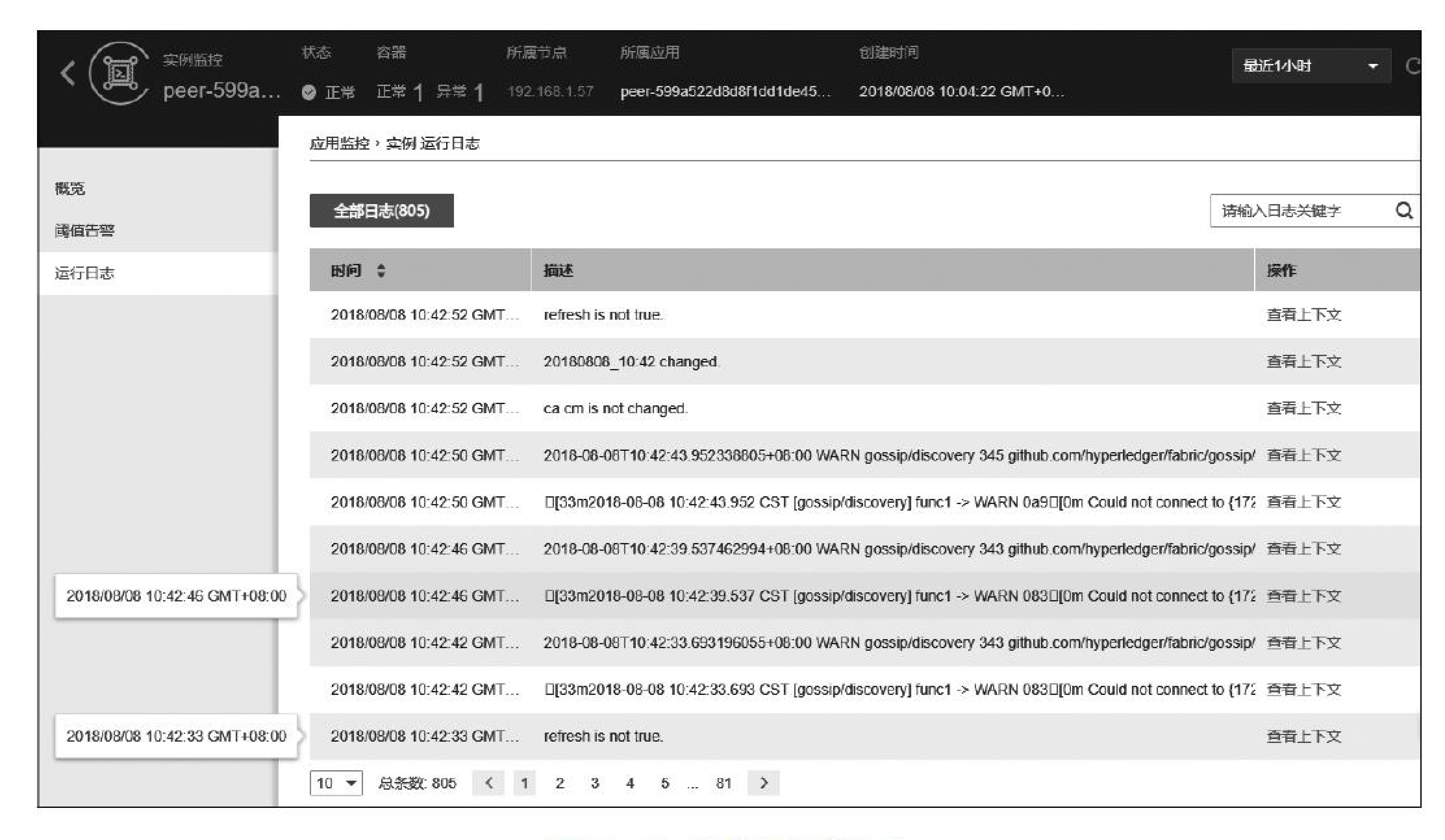
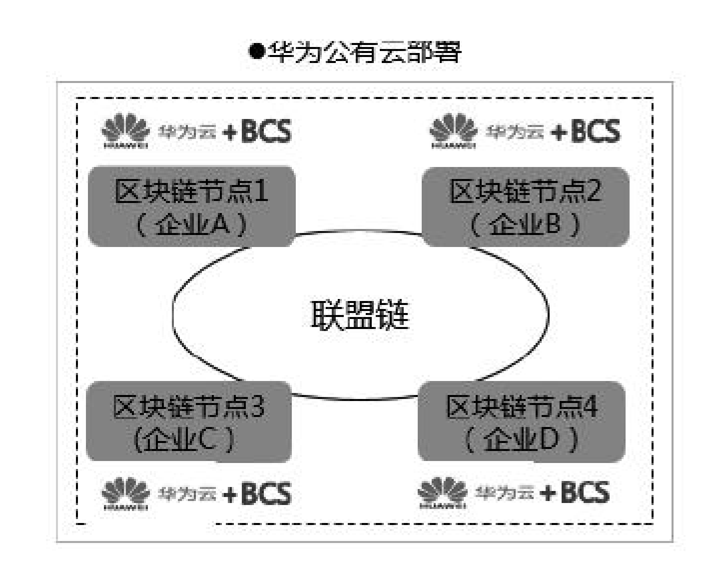


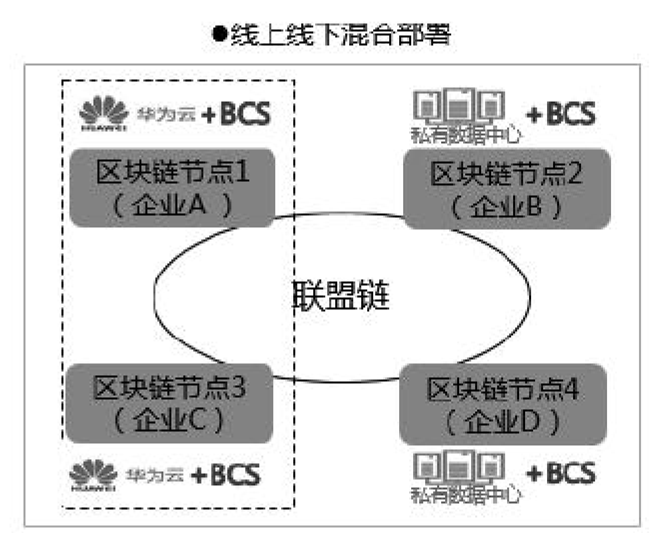
图 13.34　区块链容器日志

至此,我们的区块链服务极速之旅圆满结束。相信读者已经可以感受到华为云为开发者所想,尽心提供一站式服务的理念。相比开源平台,华为云的区块链服务不仅在前期降低了企业使用区块链的难度,更提供了一整套后期的运维保障服务,这也正好符合华为云的服务理念:让企业上云更容易。

13.4　区块链服务的跨云部署和云上云下混合部署方案

随着客户业务规模扩展到全国乃至世界范围内,基于当地的政策法规将当地业务部署到云平台时,为了和现有的业务打通,需要使用跨云部署的解决方案。在某些场景中,政府客户或者一些对数据隐私性保护严密的客户,既需要公有云平台提供的服务,又需要本地的数据私密性的需要,本地需要自己的数据中心,在这种情况下就需要依赖云上云下混合部署方案。如图 13.35 所示,就是三种部署方案的大体架构,第一种是全公有云部署,第二种是线上线下混合部署,最后一种是以 SAP 云作为例子打通 BCS 和 SAP 的混合云部署方案。本章会重点描述如何在华为云上进行线上线下和跨云打通的基本步骤。





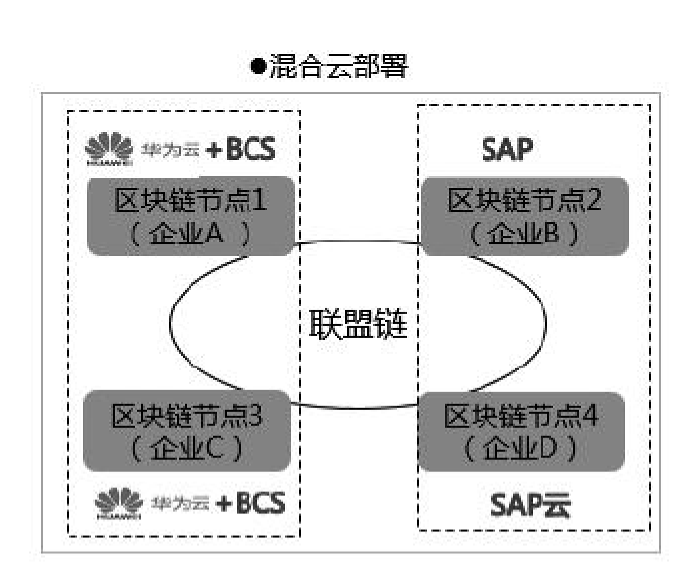


图 13.35　混合云部署方案图

不论线上线下还是混合云的方案,他们的区别在于是客户本地私有数据中心集群还是一个云上的私有集群,都需要有对外连接的地址和相关节点存在。因此,打通他们之间的步骤都是类似的,可以分为下面的三步。这里以一个客户 B 希望将自己的节点和另一个网络内部的客户 A 的节点加入共同通道为例。

13.4.1　将节点加入区块链网络

如图 13.36 所示,是客户 B 将一个节点加入客户 A 的网络中的过程。完成这个过程需要五步:

（1）客户 B 从云提供商 B 那里获取所有相关的节点信息,并生成加入请求的 json 文件;

（2）将这个请求 json 文件发送给客户 A;

（3）客户 A 收到客户 B 发送的加入网络的请求后,将其节点信息更新到自身的系统通道内部,并将自身网络信息生成响应 json 文件;

（4）客户 A 将响应 json 文件发回到客户 B 处;

（5）客户 B 将响应 json 文件中的客户 A 网络配置导入自身网络中,完成节点加入网络流程。

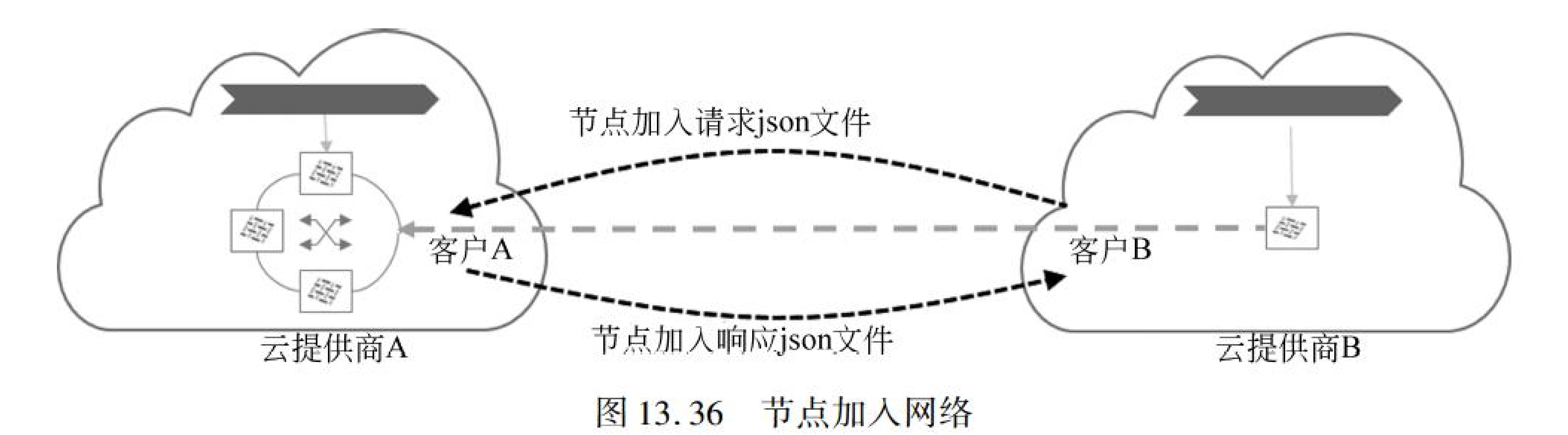


图 13.36　节点加入网络

13.4.2　加入区块链网络通道

如图 13.37 所示,客户 B 和客户 A 已经是在同一个区块链网络中后,发起请求并加入通

道的流程。由于在区块链网络中可以支持加入多个通道,所以这个操作可以重复执行。完成下面的加入通道的过程也需要五步。

(1) 客户 A 告诉客户 B 哪些通道可以加入后,客户 B 生成加入这个通道的请求 json 文件;

(2) 客户 B 将加入通道请求的 json 文件发送给客户 A;

(3) 客户 A 收到请求文件后导入自己的云网络中,然后生成通道加入的响应 json 文件;

(4) 客户 A 将响应 json 文件发送给客户 B;

(5) 客户 B 将响应 json 导入自己的云网络,完成加入通道、更新锚点等操作的整体过程。

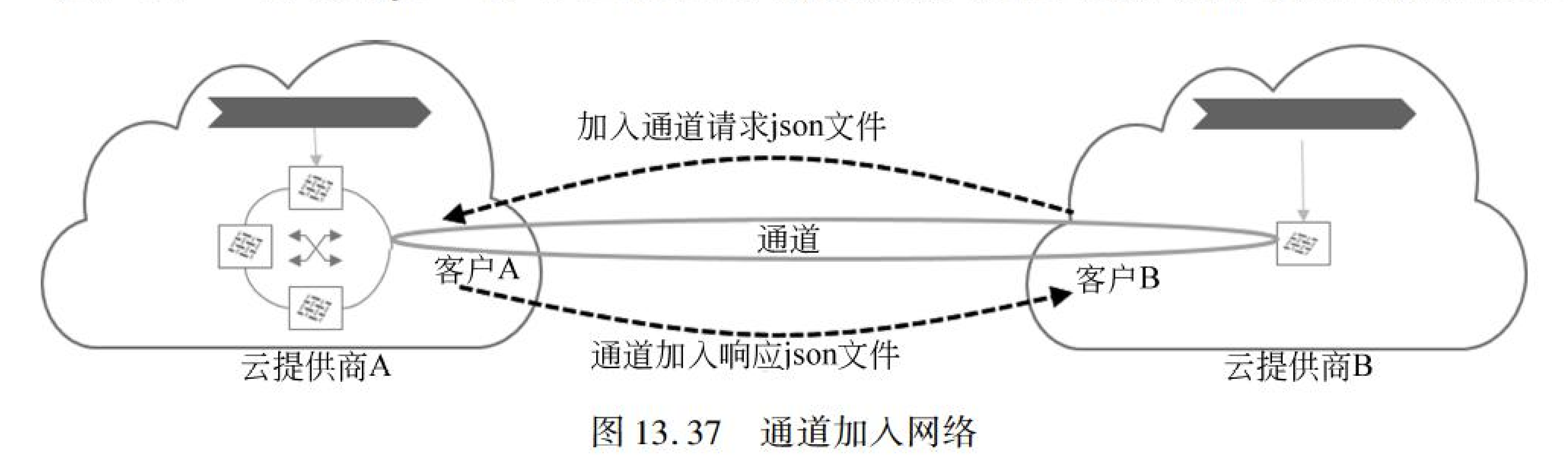


图 13.37　通道加入网络

13.4.3　部署链码到区块链网络通道中

如图 13.38 所示,客户 A 和客户 B 都可以部署和实例化链码到上一步加入的通道内。客户和不同的合作伙伴之间可以共享它们的链代码,但是链码源文件在不同操作系统拷贝相当脆弱,因此可以使用签名链码规范的标准格式生成二进制链码文件。这一步如能妥善处理代码传输,同样可以支持使用源代码文件。

(1) 客户 A 生成链码的二进制文件;

(2) 客户 A 将二进制文件发送给客户 B;

(3) 客户 B 将二进制文件上传进行安装部署。

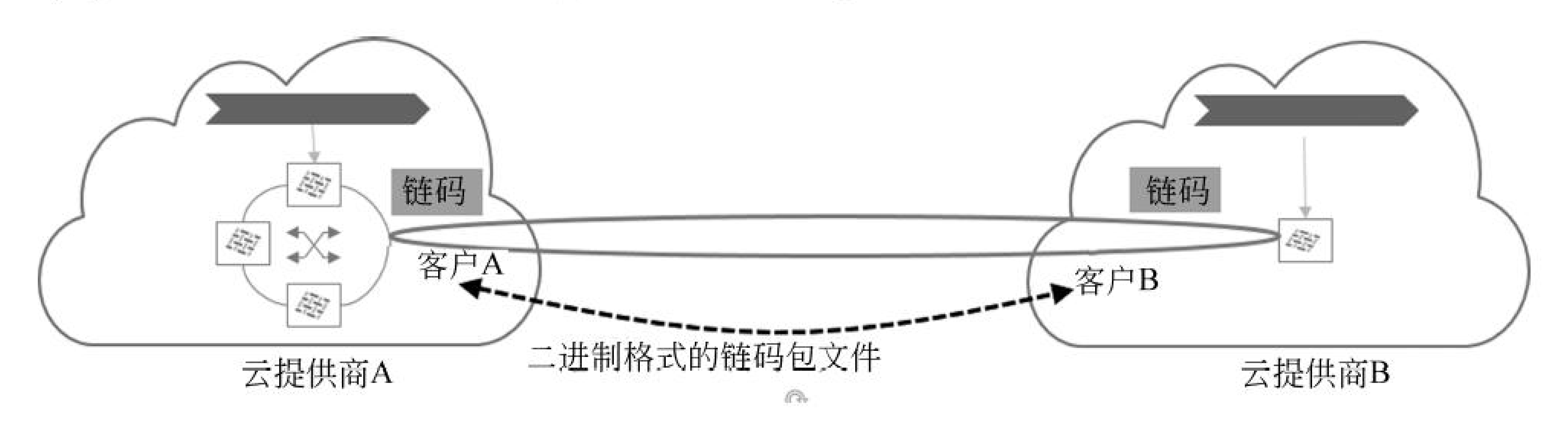


图 13.38　部署链码到区块链网络

13.5 本章小结

本章主要是面向开发人员,介绍华为公有云上的区块链服务。本章首先分析了基于公有云的区块链系统的优势所在,而后开始介绍华为云区块链服务的上手和构建。整个区块链的应用构建是从计划部署开始,到购买区块链服务进行开发,最后对整个系统进行运维。本章还扩展介绍了区块链的跨云部署和云上云下结合的模式,使读者能更加系统地了解区块链云服务的开发思路。



第三部分 区块链未来

任何技术的快速发展都离不开社会的持续关注以及资本的持续投入,从这个角度来看,区块链是幸运的。当前,区块链技术正处于快速发展演进期,基于区块链的大量应用正处于孕育阶段,区块链的未来无疑一片光明。然而,区块链也不是万能的灵药,并不是所有的业务难题都可以在区块链领域找到答案,区块链相关从业人员在面对诱惑时仍需保持理智,谨守行业道德,为区块链的长期良性发展贡献力量。

第 14 章
区块链的价值及前景

“这是最好的时代,也是最坏的时代;这是智慧的年代,也是愚昧的年代;这是信仰的纪元,也是怀疑的纪元;这是光明的季节,也是黑暗的季节;这是希望之春,也是失望之冬;我们面前应有尽有,我们面前一无所有;我们正走向天堂,我们正直下地狱。”

——狄更斯《双城记》

14.1 区块链技术的发展环境

18 世纪 60 年代,随着牛顿力学的创立和发展,以瓦特改良蒸汽机为标志,人类进入“蒸汽时代”,开始以机器代替人力,以大规模的工业生产代替个体手工业生产。

19 世纪 70 年代,电磁学从理论走向实践,发电机、内燃机、电灯等重要发明相继问世,人类进入“电气时代”,生产力得到进一步飞跃。

20 世纪中期,原子能、计算机、航空航天、生物工程等学科得到深入发展,进而带动其他高新科技的发展,人类进入“信息时代”,生产生活水平得到前所未有的提高。

第三次科技革命正如火如荼,第四次科技革命已悄然来临,以互联网产业化、工业智能化为标志,物联网、大数据、云计算、人工智能、区块链、机器人等技术得到飞速发展。第四次科技革命吸引了各国政府和科技巨头们的极大关注,各组织团体分别开展各自相关领域的基础和应用研究。谷歌、Facebook、亚马逊、苹果、华为、BAT 等巨头竞相投入机器人、无人机、无人

驾驶、医疗大脑、智能音响、城市大脑、区块链等领域。小规模应用已经初见成效，大规模应用如潜伏在海平面下的冰山，正待浮出水面。

这些技术到底是将照亮人类未来的普罗米修斯的火种，还是将会把人类推向万劫不复的深渊的潘多拉魔盒？回想一下当年人类对原子能的开发和利用，一方面创造了核武器，让人类命运一度被冷战的核阴影所笼罩，另一方面建造了核电站，为人类提供了大量的能源。一面天使、一面魔鬼，完全取决于人类如何应用。

在第四次科技革命中，区块链具有什么价值呢？我们需要从区块链解决的问题——社会关系说起。

人是社会关系的总和，有人的地方就有江湖，有江湖的地方就有纷争。纷争的本质是利益纠纷，而为了解决利益纠纷问题，人类发明了各种中介机构，也就是引入一个“公正”的第三方来解决人们之间相互不信任的问题。于是各类商业平台、支付第三方、P2P 理财、房屋中介、婚介中心等中心化的中介机构应运而生，也在一定程度上发挥了其作为一个中立第三方的作用，成就了更高效的物质或信息资源交易或交换。然而，随着市场的发展和日趋激烈的竞争，中心化中介机构的一些弊端逐渐显露。由于整个系统都依赖一个中心化的第三方来进行维护，因此当中心因为利益原因开始作恶，整个系统的公平性甚至安全性都会遭到破坏。中心作恶导致参与者蒙受损失的事件层出不穷，如 P2P 暴雷、多平台用户数据隐私泄露甚至被恶意兜售、商业平台与商家勾结欺骗消费者、婚介诈骗等，本来为了解决信任问题而引入的中心现在成了最大的信任问题。

第四次科技革命本质上是生产力的革命，生产力决定生产关系，生产关系反过来影响生产力的发展，落后的生产关系阻碍生产力的发展，先进的生产关系促进生产力的发展。第四次科技革命影响的广泛性和深刻性决定了它必然需要人人参与、人人受益，而不只是少数中心巨头们的狂欢。从人类发展的历史趋势来看，中心化的生产关系和组织方式已经不能适应生产力的飞速发展，必将越来越成为生产力发展的障碍，去中心化势在必行。

区块链是人类迄今为止去中心化和解决信任问题最具革命性的一次探索，天然具备去中心化、透明、防篡改、高效率、低成本特性，区块链从一开始就致力于解决人类信任问题，将人与人的信任转变为人与机器的信任。如果说现代社会处在契约时代，区块链将使我们进入自动契约时代，通过编码让机器代替第三方中介委托监管各种契约履约情况，既提高了效率，又避免了第三方作恶。

以人工智能为代表的第四次科技革命正获得飞速发展，如何确保它走在正确的道路上呢？人工智能还没有得到普遍应用，却已经开始暴露出各种问题，如种族歧视、性别歧视、大数据杀熟、隐私泄露等。可以想象，当物联网的触角延伸到人类活动的各个角落，人工智能算法深度参与到医疗、法律、服务，甚至立法、行政、警察、军事等领域后，这些问题只会更加严重。我们不得不及早准备，防患于未然。应用区块链技术打造可信计算及可信信息传递或许是解决这些问题的一种途径，甚至是目前为止最有希望成功的一条路。因为问题的根源是信任问题，而区块链正是为解决信任问题而生。

我们不妨畅想：未来的某一天清晨，你家的机器人助理根据你以往的作息规律轻声唤醒了你，它说已经准备好早餐并摆好餐桌。你吃早餐的时候，大屏幕上传来奶奶急切的呼唤，你知道一定又是催婚，你叹口气却无可奈何。而机器人助理已经根据你的性格爱好筛选了几个合适的对象，并且从学历区块链、诚信区块链证实了信息的真实性。你让机器人助理帮你约了其中一个中午 12 点一起吃午餐。大屏幕闪动两下，老板光头强正冲着你大吼大叫，叫你赶紧把一份绝密文件发到客户熊二的邮箱，你通过公司内部区块链确定这条讯息是真实未被篡改的，公司通信软件已经自动将光头强的这条指令附加上指纹和电子签名上链。你走在各种智能体匆匆忙碌的第五大街上，享受温暖明媚的阳光，感叹科技真好，因为你知道一切都是安全的、可追溯的，底层的区块链系统正记录并分析整个世界的流动，这是一个智能又安全的世界，全民参与，全民见证。

第四次科技革命将推动人类进入"智能时代""可信时代"，未来已来！

14.2　区块链缩短了信任的距离

纵观人类近代生活方式的改变与进步，无不与科学技术的发展有着直接的关系。巧合的是，每一次变革都伴随着某种意义上的"距离"坍塌，而这些变革正在一定程度上缩短了某种"距离"，为人们带来了便利。

如图 14.1 所示，交通工具的出现，缩短了人们在地理上的距离。俗话说要致富、先修路，就说明了交通的便利与生活水平的提高之间的必然关系。当地理的距离缩短之后，人们的需求又上升到了信息的层次。一开始我们使用信件、电报交换文字信息，然后发展到使用电话交换语音信息，紧接着随着互联网的兴起，数字信息的壁垒被彻底打破，我们不再畏惧信息的形式，有互联网作为载体，我们可以便利地以各种形式交换信息数据，生活的便利性大大提高。然而，便利的互联网也带来了信息量的高速膨胀，人们在面对海量的信息时，很容易陷入迷茫，难以获取真正需要的信息。人工智能的出现解决了人们面对海量信息的困惑，海量数据非但没有成为负担，反而为人们认知世界提供了新的契机，这恰恰缩短了认知的距离。不过，此时人们获得有效信息依然要依赖各类中间机构对信息的收集和整理，单纯的人与人之间往往难以有效、可信地获取信息。在这样的背景下，区块链技术应运而生，因为中心化架构存在着天然的不平等性，这一定程度上限制了人们得到公平对待的权利。区块链技术正是以解决人们信任的距离为目标，在区块链网络里，人人平等，所有信息开放、透明、可追溯、不可篡改，人们可以在没有任何中心机构存在的前提下实现价值交换，人与人之间的交互得以进一步简化。



图 14.1　科技变革缩短了距离

14.3 区块链的价值及前景

基于中心化的组织或机构构建的信用体系是传统商业社会的基础。区块链技术出现之前,人们无法构建一个行之有效的去中心化大规模信用系统。以比特币为代表的区块链技术的社会化实验,首次实现了真正去中心化的价值交换系统,保证了数字货币交易系统安全、稳定地长期运行。随着区块链技术的快速发展,其必将在更多领域、更深层次地影响和改变商业社会的发展。区块链技术对商业社会的影响具体体现在以下三个方面。

1. 降低社会交易成本

区块链系统的去中心化特征,决定了所有的交易均由参与方通过共识机制建立分布式共享账本,参与方通过区块链网络对交易内容进行提交、确认、追溯等操作。换言之,区块链网络中的所有信息都是经过多方共识、可信、不可篡改的。这将极大简化传统交易模型中所要面对的冗长的交易审查、确认等流程,甚至不再需要重复的账目核对、价值结算、交易清算等操作,从而实现社会交易成本的大幅降低。

传统的社会交易往往依赖人与人之间的信任或人对第三方机构的信任,然而这种信任是不安全的,因为即便是正规的法律合同,在执行过程中也难免存在灰度部分,可能会导致交易参与方的权利和义务不能得到充分的保障。区块链技术中智能合约的提出,是这一问题的有效解药,通过在交易协商过程中将合约内容“代码化”,区块链系统将为整个合约的执行负责,保证交易执行的有效性和参与方的合法权益。

2. 提升社会效率

随着区块链技术应用于经济社会的各个领域,必将优化各领域内的业务流程,降低运营成本,提高协同效率。以金融领域内的场景为例:当前金融系统是一个复杂庞大的系统,跨行交易、跨国汇兑往往需要依赖各类“中介”组织来实现。漫长的交易链条,加之缺乏统一的监管方式,使得交易效率低下,大量资产在交易过程中被锁定或延时冻结。而借助区块链系统实现的去中心化体系,社会中的投资和交易将可以实现实时结算,这将有助于大幅提升投资和交易效率。扩展场景到其他领域,各类需要依赖“中介”来解决信任问题的场景,或者依赖来回核对来解决信息一致的场景,都可以使用区块链技术作为其解决方案,可以大大减少操作步骤以及人力投入,降低对中心化机构的依赖,提升效率。

3. 交易透明可监管

信息的实时性及有效性是监管效率的关键。除了涉及个人隐私或商业机密等情况外,区块链技术可以实现有效的交易透明、不可篡改特性,监管机构还可以实现实时的透明监管,甚至可以通过智能合约对交易实现自动化的合规检查、欺诈甄别等能力。

互联网技术一直以来均处于高速发展状态,为人们带来了巨大的便利,也给人们的生活方式带来了巨大的革新。而细观区块链技术的发展历程,又与互联网何其相似!

从表 14.1 可以看出区块链的更新与发展和互联网呈现出极其相似的周期性变化规律。

不同的是,区块链的周期更小,迭代更快。

表 14.1　区块链与互联网发展历程对比

互联网(10 年尺度)	区块链(5 年尺度)
1974—1983 年 • ARPANet 试验网络	2009—2014 年 • 比特币试验网络
1984—1993 年 • TCP/IP 基础协议确立 • 可扩展基础架构完成	2014—2019 年 • 超级账本、以太坊等 • 基础协议和框架探索
1990—2000 年 • HTTP 开始被应用 • 正式向商用领域开放	2018—2023 年 • 核心协议探索中 • 商业应用加速
2000— • 互联网普及	? • 商业协同网络

互联网的发展历程是科学技术飞速发展的历程,也是生产力和生活水平迅猛提高的历程,科学技术是第一生产力的论断在科学技术和生产实践中得到了充分检验。从技术发展的角度看,区块链是互联网技术的发展和延续,如果把互联网比作信息之路,那么区块链的目的就是为它加上红绿灯、照明设施、信号标志等,让信息之路更安全更可信赖。互联网技术实现的是信息流通,而区块链实现的是价值流通,信息流通通过半自动化提升了生产生活效率,而价值流通则将和机器智能、IoT 等技术一起实现全自动化,必将进一步推动生产力发展。从发展趋势看,互联网将向着高速、可信、万物互联、智能化的方向发展,其代表性的技术方向分别是 5G、区块链、IoT、机器智能。互联网是区块链的基础,作为多方可信计算落地的区块链是互联网的发展和延伸,是互联网从信息高速公路向价值高速公路升级的必然结果。

我们当前正处于 2018—2023 年这一时间跨度之内,从业人员正在积极探索核心协议,并且加速落地商业应用。在这一阶段,区块链技术将会日益成熟,而区块链可以应用的行业领域将有更多的探索,届时区块链也将如互联网一样深入人们的生活,改变人们的生活习惯。而未来,“万物互联”将不再是一个口号,区块链以其去中心化、传递信任的特性和能力,将作为最底层的通信协议撑起未来的网络通信,区块链终将成为人们生活中不可或缺的一部分。

14.4　本章小结

本章从未来发展角度分析区块链的核心价值。如果说 20 世纪末半导体、互联网和核能等技术是第三次工业革命的话,那么在不远的未来,很有可能区块链技术将与人工智能、物联网和量子计算等一起,成为第四次工业革命的中坚力量。如果社会的进步带来的是社会分工的不断细化,那么区块链技术在这个需要大规模协作的社会将重构原有的信任关系,拉近信任的距离。最后,本章从交易成本、协作效率和监管等方面分析了区块链的价值,使读者对于区块链的核心价值有更深刻的理解。

第 15 章
区块链的其他声音

随着区块链技术的发展与众多区块链系统的上线,区块链正在越来越多的领域被应用。然而,当前大众对区块链技术的理解存在一定误区,要么认为区块链技术对溯源一无用处,要么将这一技术神化,认为其无所不能。因此,对区块链技术的认识还是应该趋于理性,客观地认识到其突破性和局限性。本章将社会上对区块链技术的一些认识和应用趋势进行介绍,使读者能更客观理智地了解区块链技术的应用前景。

15.1 区块链能否完全解决溯源问题的争议

当前区块链溯源已经被认为是区块链技术的一大应用。区块链技术的确可以很好地应用于溯源,在一定程度上保证资料来源和变动历史的可信性,但它解决不了源头信息造假的问题,即业界常说的,链上数据不可篡改,但上链原始数据是需要人来进行输入,即由人控制的。

15.1.1 区块链溯源技术的应用

区块链溯源是利用区块链技术,通过其独特的不可篡改的分布式账本特性,对物品实现从源头的信息采集记录、原料来源追溯、生产过程、加工环节、仓储信息、检验批次、物流周转到第三方质检、海关出入境、防伪鉴证的全程可追溯。其基本功能结构如图 15.1 所示。

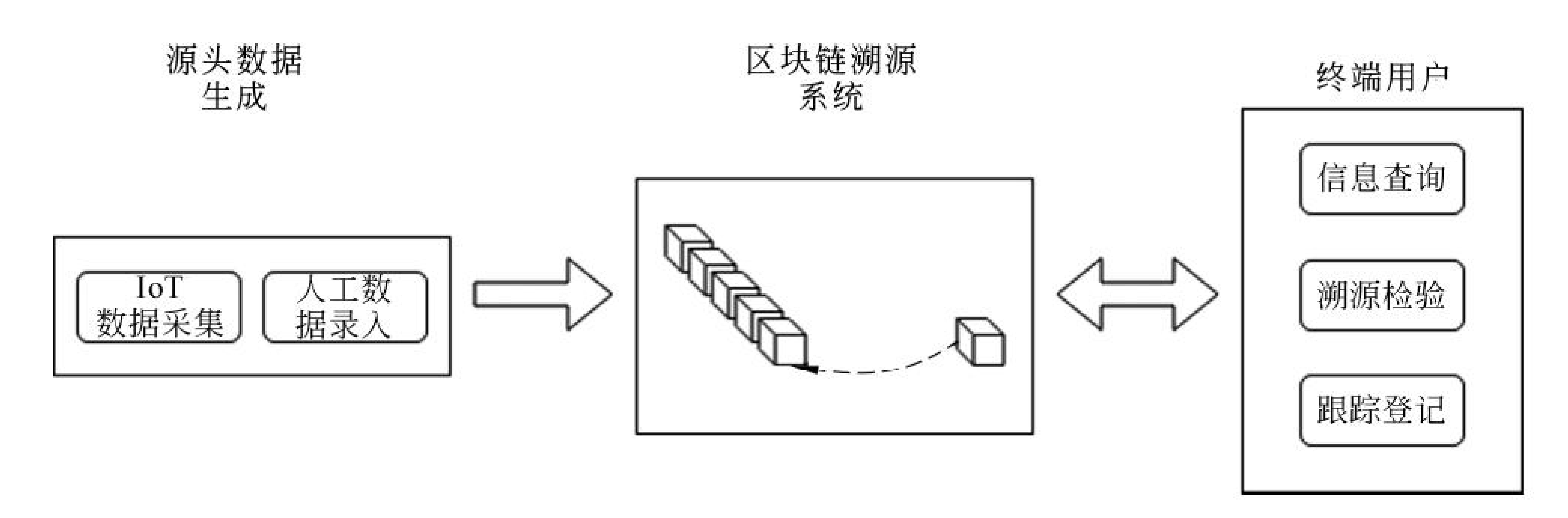


图 15.1　区块链溯源系统框架

区块链溯源系统流程包括：

(1) 首先通过溯源数据生成系统,从真实货物生成原始数据,一般使用 IoT 数据采集方式或人工录入方式；

(2) 将原始数据进行处理后,传入区块链溯源系统,一旦数据进入此系统,整个系统使用区块链技术来保护数据,信息得到保证,不可篡改；

(3) 包括供应链、最终用户等的终端用户对数据更新及使用。

其中步骤(2)和步骤(3)会对数据进行更新操作,能通过区块链技术实现去中心化的、不可篡改的信息存储,从而解决信任问题。但是,步骤(1)作为数据入口,如何保证信息采集或者数据录入正确还有待解决。接下来我们看两个典型的应用案例。

(1) 区块链食品

当前市面上出现了不少以区块链命名的商品,这类商品通常是想借助区块链技术来为自身商品作背书,其主要目的是使用户可以通过区块链技术对商品进行溯源,从而了解商品生产加工过程中每个步骤的关键信息,并通过此技术来对商品进行防伪。然而实际上,商品生产商想让用户看到的商品相关数据,仍可进行一定程度的造假。举一个例子,A 产地的黄桃很出名,销售商通过区块链技术为其背书,将该批次的黄桃信息,如产地、大小尺寸、保鲜期及相关信息上传到区块链,中间二次加工等过程信息也上传链,宣称通过区块链技术实现溯源以保证品质,但该批次的黄桃真是 A 产地的吗？还是从 B 产地调往 A 产地？这些线下操作,完全由人为参与控制,上传到链上的数据有真有假,对于用户来说,根本无法分辨这些数据的真假,也就实现不了真实的溯源。

(2) 区块链钻石

某钻石生产商声称正在试验使用区块链技术追踪钻石从开采到零售的整个流通过程。在刚结束的试验中,该公司成功追踪了上百颗高价值宝石在切割、抛光和制造等各个环节中的流通情况,并使这批宝石的质量管控取得了显著的效果。

此类商品,从毛坯开采、切割、批发和零售到加工后流通到消费者手中,这其中还需要通过鉴定开具证书、跨境交易报关进出口、外汇结算等环节,过程相当复杂,交易过程中的规则

和监管环节多,也容易出现问题,因此区块链的应用对物品追溯、自证清白就显得相当重要,消费者对自己购买商品的了解和后续服务操作等,都可以通过区块链技术获得更好的服务;总体来讲,主要是想通过区块链技术的特点来实现商品在整个供应链上的跟踪与溯源,以起到“打假”、质量保证、品牌保护等效果。

15.1.2 区块链溯源面临的挑战

溯源技术主要是指用于跟踪产品在供应链自上游至下游的生命周期状态及可以从产品的某个下游状态回溯至其来源处的技术。我们可以总结溯源系统是利用物联网、大数据建立的一套完整体系,使得产品从生产过程到流通环节的信息都能追溯可查。

早在 20 世纪 90 年代,“溯源系统”就被欧盟提出并建立,当时主要用于应对“疯牛病”,通过此举逐步建立并完善其食品安全管理制度。最早的溯源系统是为了解决农产品等食品安全问题,试图从源头控制好食品质量。同时,溯源系统不仅仅可用于追溯源头,它还实现了对物品流转过程进行全程的跟踪。例如对各类艺术品、古迹、奢侈品在全世界流转的过程进行追踪、或对商品在流通环节的处理过程进行记录等。

当前,传统的溯源系统还存在一些问题,主要表现在:

(1) 为商品生成防伪码时,如何鉴别商品本身的信息?很多商品从源头开始追踪,跟踪信息等都靠人工记录,不光浪费时间,同时这过程中很难保证信息的真实性,从而产生信用问题。其次,尽管现在有较多防伪形式,如条形码、二维码、射频识别等,但其仍存在可能被复制、盗用的风险。

(2) 溯源信息系统的数据管理中心,有可能存在人为作恶修改数据的可能性、黑客攻击等问题,信息同样无法得到保障,最终还是面临着一定程度的信任问题。

综上所述,区块链在溯源技术中的应用能够使溯源过程中的信息整合、流通、共享更加便捷和透明,能够在一定程度上助力溯源技术。然而,源头数据“上链”的过程中的真实性和正确性的保证与区块链技术本身无关。可以说,区块链技术能够限制信息流通过程中的造假行为,提高造假成本。但若要完全解决信息源头造假问题,还需要结合区块链技术以外的防伪手段。例如,可在信息上链之前增加专业机构的验证环节对上链信息进行认证,或通过物联网进行自动化的信息采集从而排除信息上链过程中人工干预的可能。通过这些额外的防伪手段,可对信息源头造假问题进行一定程度的控制和防止,从而打造更可靠和完善的溯源解决方案。

15.2 加密数字货币及 ICO 所带来的影响

加密数字货币,有时简称加密货币,是一种使用密码学原理来确保交易安全及控制交易单位的交易媒介。加密数字货币是数字货币(或称虚拟货币)的一种。其中,比特币在 2009 年成为第一个去中心化的加密数字货币,这之后加密数字货币一词多指此类设计。加密数字

货币基于去中心化的共识机制，与依赖中心化监管体系的银行金融系统相对应。

ICO 意为首次加密数字货币发行，源自于股票市场的首次公开发行 IPO 概念，是区块链项目首次发行代币、募集比特币或以太坊等通用加密数字货币的行为。原本 ICO 概念限于对区块链技术应用项目开发，发行的代币主要用于对技术开发人员奖励，本质上更接近于技术开发项目的早期众筹。国际上，ICO 的项目发行形式主要是以慈善基金的形式，购买代币可以理解为一种“捐赠”行为，以此来“资助”相关项目的早期研发，全球 ICO 项目 TOP 如表 15.1 所示。

表 15.1 全球 ICO 项目 TOP7 占比

United States	15.98%	Switzerland	6.60%
United Kingdom	9.53%	Estonia	4.11%
Singapore	8.36%	Australia	3.37%
Russian Federation	7.04%		

注：数据来源于 https://icowatchlist.com/statistics/geo

由于基于区块链的加密数字货币不受政府等相关机构的严格管控，近年来 ICO 现象迅速升温，新型网络众筹模式更是在中国迅猛发展。不过，新增项目大多与区块链技术关系不大，一些唯利是图的非法组织也乘虚而入，仅是希望借着概念发行代币获利，迅速催生了泡沫。

2017 年 9 月 4 日下午，中国人民银行、中央网信办、工业和信息化部、工商总局、银监会、证监会和保监会联合发布了《关于防范代币发行融资风险的公告》。该《公告》宣布了取缔 ICO 的决定，明确指出，包括 ICO 的代币发行融资“本质上是一种未经批准的融资行为，涉嫌非法发售代币票券、非法发行证券以及非法集资、金融诈骗、传销等违法犯罪活动”。

在央行发布公告后，各大代币全线崩跌，一天蒸发数亿。目前 ICO 发行方多数在清退代币，但也有部分发行团队或不法分子已将资产、资金转移，可能造成 ICO 投资人的巨大损失。

近几年，随着区块链技术的全球性兴起，加密数字货币作为区块链技术的典型应用项目，充斥着各个行业每个角落。据粗略统计，目前市场上已经有接近千种加密数字货币，如比特币、莱特币、以太币、瑞波币等。比特币、以太币等较为成熟的，并具有一定技术积累的项目已经有了深厚的用户基础，然而一些后发行的币，几乎濒临死亡，其中不乏以圈钱为目的的劣质币。

根据中国国家互联网金融安全技术专家委员会发布的报告，仅 2017 年上半年，ICO 累计融资达到 26.16 亿元人民币，累计参加人次约 10.5 万。相比火爆的交易活动，关于 ICO 的管理制度则几乎为空白，由此也导致市场乱象频现，投机活动泛滥。大多数非法 ICO 为私人公司或者个人对公开的区块链程序进行修改后，以新发代币的形式面市，以达到吸引民众投资的目的。这些非法 ICO 跟以往所有的庞氏骗局一样，在经历过初期价格快速上涨之后，到最后就要看击鼓传花谁接最后一棒，泡沫很快破裂，投资者往往血本无归。

由于非法 ICO 由私人发行，私人平台进行交易，独立运行于国家监管体系之外，会大量滋生洗钱、逃税等非法金融行为。主要的影响归结为以下两方面，一方面，受到比特币等不少热

门区块链代币的影响,众多进行非法 ICO 的私人公司和私人平台,在短时间内圈完钱就跑路,最终受伤的大多是普通老百姓,进而产生不少的社会问题;另一方面资金大量参与 ICO,对实体经济和金融体系形成抽血,并影响货币政策传导,使宏观调控效果失真,影响宏观决策。

加密数字货币市场是一个面向全球、尚未纳入严格监管的另类金融市场,其规模虽然仍然较小,但其野蛮生长和缺乏全球监管协调的现实,给全球金融市场带来了新的风险因素。有必要就加密资产和数字货币问题加强政策协调。不过需要说明的是,加密数字货币仅是区块链技术的一类应用,不应因加密数字货币市场所带来的混乱而对区块链技术本身持怀疑态度。实际上,各国政府对加密数字货币和区块链技术本身的态度往往是完全不同的。

15.3 各国政府对待加密数字货币及区块链的态度

随着比特币、以太币等加密数字货币的大热,各种加密数字货币如雨后春笋般蓬勃发展。尽管各国政府对区块链技术都持正面态度,积极鼓励并推动其技术发展,但对待加密数字货币的态度却截然不同,有些国家将其视为未来发展不可或缺的一部分而设立相关法规进行保护、鼓励,而有些国家视其为非法而立法禁止,也有部分国家对此持中立态度。总体来说大部分国家对加密数字货币持乐观态度,下面让我们看看几个代表性国家的态度是怎样的。

(1) 中国

中国对加密数字货币整体持慎重态度,相关法律法规的发展时间表如下。

- 2016 年 3 月 10 日,中国人民银行行长表示,加密数字货币均非法定数字货币,建议各位投资者不要购买。
- 2017 年 9 月 4 日,央行等七部门联合出台严令,以 ICO 融资为代表的代币发行融资被叫停。
- 2017 年 9 月 15 日,监管部门全面叫停加密数字货币交易平台,要求各平台于 9 月 30 日关闭所有交易功能。
- 2018 年 2 月 5 日,中国银行表示:“我们不接受任何关于加密数字货币的交易,中国将不会打开加密数字货币的市场。”
- 2018 年 3 月 9 日,原央行行长周小川表示,加密数字货币还处在摸索阶段,加密数字货币未来监管取决于技术成熟程度及测试评估情况,还有待观察。同时他坦言,中国对加密数字货币仍持开放态度,但前提是它不会破坏金融系统,实施动态监管。由此,中国加密数字货币仍处于严监管状态。

然而对于区块链技术,我国政府与企业则表现出浓厚兴趣并且支持发展区块链技术。目前,各地政府纷纷启动区块链创新项目,以期将区块链技术应用在政府公共管理和企业创新中,提高政府、企业效率。

(2) 美国

美国政府对加密数字货币持积极态度,同时也加强了对加密数字货币交易的监管,遏制

与之相关的洗钱和恐怖主义融资活动。其相关法律法规的发展时间表如下。

- 2013 年 8 月,美国德州联邦法官 Hirsh 把比特币裁定为合法货币,受《联邦证券法》监管。
- 2014 年 6 月,加州州长签署的 AB129 法案指出,包括加密数字货币、积分、优惠券在内的美元替代品为合法货币。
- 2014 年 12 月,纽约将加密数字货币管理和比特币牌照相关法规纳入《纽约金融服务法律法规》,启动对比特币的监管。
- 2015 年 1 月,纽交所入股的 Coinbase,获批成立比特币交易所,美国以纽约州为代表的比特币监管立法进程初步完成。
- 2017 年 2 月,美国亚利桑那州通过区块链签名和智能合约合法性法案。
- 2018 年 3 月 9 日,南卡罗来纳州发布停止令,暂停云采矿服务公司 Genesis Mining 以及 Swiss Gold Global 公司在美国南卡罗来纳州的运营。
- 2018 年 3 月,美国国会发布《2018 年联合经济报告》,报告专门有一个章节讨论加密数字货币和区块链。

对于区块链技术,美国也表现出了浓厚的兴趣和支持态度,在 2018 年 2 月 14 日,美国众议院召开第二次区块链听证会,将区块链上升到“变革性技术”,探讨的应用场景涵盖了金融、商业和政府效率提升等方向。

(3) 韩国

韩国对加密数字货币的态度由最初的禁止交易逐渐转变为积极支持,其相关法律法规的发展时间表如下。

- 2017 年 9 月,韩国政府制定了全面禁止 ICO 的禁令。
- 2018 年 1 月 12 日,韩国准备立法禁止数字货币交易,4 万民众请愿罢免金融监管局主席。
- 2018 年 1 月 23 日,韩国信用卡禁止向海外加密数字货币平台兑换交易。
- 2018 年 1 月 31 日,韩国法院裁定比特币可以通过交易所兑换成货币,它可以作为一种通过商家支付的手段,因此它应该被视为具有经济价值。
- 2018 年 2 月,韩国金融监督管理局再次发出积极信号,强烈呼吁韩国加密数字货币的发展和“正常化”。
- 2018 年 3 月 13 日,据《韩国时报》报道,韩国政府或很快取消对 ICO 的禁令,允许一定条件下的代币销售。
- 2018 年 7 月 30 日,韩国政府发表《2018 年税务法律改政案》,在对于初创公司和中小型公司减免税务对象中不包括加密资产买卖与中介行业(虚拟货币交易所)。韩国政府希望通过此次决定降低虚拟货币热潮,并将交易更加透明化。

(4) 日本

日本对加密数字货币的态度比较积极、开放,日本是较早将比特币等加密数字货币合法

化的国家之一。但自 2018 年 1 月 CoinCheck 被黑客盗取价值 5.23 亿美元的加密数字货币后监管趋严,对待 ICO 是默许的态度。其相关法律法规的发展时间线如下。

- 2016 年 5 月 25 日,日本国会通过《资金结算法》修正案(已于 2017 年 4 月 1 日正式实施),正式承认加密数字货币为合法支付手段并将其纳入法律规制体系之内,从而成为第一个为加密数字货币所提供法律保障的国家。
- 2017 年 3 月,日本通过了《关于加密数字货币交换业者的内阁府令》,宣布正式承认比特币作为法定支付方式的地位。
- 2017 年 4 月 1 日,日本政府宣布,承认加密数字货币的合法支付地位,所有投资者将会受到法律保护。
- 2017 年 7 月,在日本兑换比特币将不再征收 8% 的消费税。
- 2017 年 11 月,日本政府发起 ICO,振兴地方经济。
- 2018 年 3 月 8 日,日本金融厅连发 8 道"肃清令",成立"加密数字货币交易从业者研究会",整顿加密数字货币市场。

(5) 俄罗斯

与其他对加密数字货币接受程度较高的国家相比,俄罗斯对加密数字货币的态度经历了由消极到谨慎的转变的。俄罗斯将加密数字货币定义为非法货币,并因此成为比特币最大的受限市场之一。

- 2017 年 9 月,俄罗斯央行以"风险高、时机不成熟"为由,发布对加密数字货币的警告。
- 2017 年 11 月,俄罗斯正式宣布关闭比特币交易网站。
- 2018 年 1 月 12 日,俄罗斯开始起草加密数字货币交易合法化草案。
- 2018 年 2 月 3 日,俄罗斯敦促欧亚联盟(EAEU)协同应对加密数字货币。
- 2018 年 3 月 11 日,俄罗斯完成《数字金融资产》(*On Digital Financial Assets*)联邦法律的初稿,旨在对加密数字货币和 ICO 进行监管。

尽管俄罗斯政府加密数字货币整体持谨慎态度,但其对区块链技术充满热情。目前,俄罗斯中央银行称将组建工作小组,旨在分析金融市场中的先进技术和创新技术,首要研究对象包括区块链技术、移动技术和支付技术等。

总的来说,各国对于数字货币的态度各有不同,然而对于区块链技术则都呈热情拥抱和积极发展的态度,均在积极引导国内区块链技术的研究和产业化。

15.4 应用安全事故频发带来对区块链技术的质疑

截至目前,部分数字货币平台或交易所发生过若干起安全事故,由此引起了部分用户对区块链技术安全性的质疑,比如 The DAO 事件、Bitfinex 遭黑客攻击事件、Parity 多重签名钱包被盗事件、Youbite 交易所被入侵事件等,然而这些事件大多是由于部分交易所、交易平台、区块链应用及周边工具或部分劣质币开发者在开发过程中不够谨慎,引入了较多漏洞导致的,

实际多数区块链平台以及区块链技术的安全性还是具有一定保证的,很少发生事故。区块链技术的安全性有理论保证。下面我们对几个较为著名的与数字货币相关的安全事件进行简单的介绍。

(1) The DAO 事件

DAO 是 Decentralized Autonomous Organization(分布式自治组织)的简称,The DAO 是一个基于以太坊区块链平台的、当时世界上最大的众筹项目,其目的是让持有 The DAO 代币的参与者通过投票的方式共同决定被投资项目。整个社区完全自治,并且通过代码编写的智能合约来实现。2016 年 5 月初,以太坊社区的一些成员宣布了“The DAO”的诞生,该项目于 2016 年 5 月 28 日完成众筹,共募集 1 150 万以太币,当时的价值达到 1.49 亿美元。

The DAO 事件是指由于 The DAO 的部分智能合约代码在编写时不够谨慎,存在漏洞,而在 2016 年 6 月 17 日,黑客利用该漏洞盗取了 The DAO 项目的 360 多万个 ETH,按照当时的以太币价格,损失达到了 6 000 万美元。

被黑客攻击后,为了找回被盗的巨额数量以太币,以太坊社区对解决方案进行了商讨。首个提议方案为进行一次软分叉,不会有回滚,不会有任何交易或者区块被撤销,但将从块高度 1 760 000 开始把任何与 The DAO 和 Child DAO 相关的交易认作无效交易,以此阻止攻击者在 27 天之后提现被盗的以太币。但由于软分叉产生的争议与负面影响,并没有实施。最终通过一次硬分叉找回了被盗的以太币,但也导致以太坊分裂出 ETH 和 ETC(旧版)。The DAO 事件在币圈引起了巨大争议,其影响延续至今。

本质上讲,The DAO 是基于以太坊平台开发的众多应用之一,而其被攻击的事件是由于其本身的智能合约代码编写出现了漏洞,这是典型的应用开发漏洞。

(2) Bitfinex 遭黑客攻击事件

Bitfinex 是交易比特币、以太币和莱特币等加密数字货币的最大交易所之一。根据 Bitfinex 在 2016 年 8 月 2 日凌晨发布的公告,该交易所发现了自身的一个安全漏洞,并暂停了其平台上的交易。实际上,Bitfinex 负责社区和产品开发的主管塔克特(Zane Tackett)证实,该安全漏洞已导致 119 756 个比特币遭窃。以当时的价格计算,失窃的比特币价值约 6 500 万美元,可以说是一笔巨大的损失。受此消息影响,全球比特币价格应声下跌 25%。随后 Bitfinex 官网发布公告称,这次损失将由平台上所有用户共同承担,这将导致 Bitfinex 交易所内的每位用户平均蒙受约 36% 的损失。

(3) Parity 多重签名钱包被盗事件

Parity 是一款多重签名钱包,是目前使用最广泛的以太坊钱包之一,其创始人兼 CTO 是以太坊前 CTO 暨黄皮书作者 Gavin Wood。在 2017 年 7 月 19 日,Parity 发布安全警报,称其钱包软件 1.5 版本及之后的版本存在一个漏洞。据该公司的报告,截至安全漏洞被发现,已确认有 150 000 ETH(当时大约价值 3 000 万美元)被盗。据 Parity 公告所述,该安全漏洞是由一种叫作 wallet. sol 的多重签名合约出现问题导致的。后来,白帽黑客找回了大约 377 000 个受影响的 ETH,然而剩余的 ETH 也造成了平台和用户的巨大损失。同时,本次攻击导致了以太币

价格的震荡,Coindesk 的数据显示,该事件曝光后,以太币价格一度从 235 美元下跌至 196 美元左右。此次事件主要是由于合约代码不严谨导致的,受到影响的合约代码均为 Parity 的创始人 Gavin Wood 写的 Multi-Sig 库代码。通过分析代码可以确定核心问题在于越权的函数调用。实际上,区块链平台的智能合约接口必须经过精心设计,明确定义其访问权限。或者更进一步说,合约的设计必须符合某种成熟的模式或标准,合约代码部署前最好交由专业的机构进行评审。否则很容易导致各类漏洞,从而造成巨额损失。

(4) Youbite 交易所被入侵事件

在 2017 年 12 月 19 日,韩国数字货币交易所 Youbite 宣布在当天下午 4 时(北京时间 3 时)左右,交易平台遭受黑客的入侵,造成的损失相当于平台内总资产的 17%。此家平台是韩国一家市场份额较小的数字货币交易平台,在当年 4 月,这家平台就已经遭受过黑客的攻击,并且损失了近 4 000 个比特币。Youbite 表示,在 4 月份遭遇黑客攻击之后,平台加强了安全策略,并将剩余的 83% 交易所资金都安全地存放在冷钱包里。尽管如此,运营该交易所的公司 Yaipan 还是于不久之后申请了破产,并停止了平台交易。

综上所述,即使当前多数区块链平台本身的运行都十分稳定,底层技术足够可靠,但是并不能保证交易所自行开发的交易程序和用户基于区块链运行平台开发的智能合约程序的安全性。针对该现状,业界已开始针对智能合约的安全性提出各类解决方案,例如在智能合约真实部署运行前,进行安全漏洞扫描及检测,尽可能地将问题提前找到并解决。

实际上,任何技术的发展必须接受市场的检验,特别是区块链这类涉及金融等相关产业的技术,必须提供更加安全及有效的解决方案,才能更大地发挥技术本身的作用,对相关行业产生更为深远的影响。

15.5 本章小结

硬币有正反两面,所有事物也都具有相应的优势和潜在的风险。当有人宣扬区块链的颠覆性的时候,就必然有质疑和反对区块链的声音。本章对目前社会上一些较有争议的区块链应用方向进行了介绍,如区块链在溯源领域的应用、数字货币相关的 ICO 乱象等,分析了其产生的根本原因;同时本章也对各国政府对于数字货币及区块链的态度进行了介绍。总的来说,尽管各国政府对于加密数字货币的态度并不相同,抛开加密数字货币而言,各国政府对于区块链技术均是大力支持并积极发展的。在本章的最后,我们对加密数字货币领域发生的各种安全事故,比如 The DAO 漏洞和加密数字货币被盗等进行了介绍,同时分析了这些漏洞与区块链技术本身的关系,帮助读者更好地辩证看待区块链技术。

第 16 章
区块链发展趋势

16.1　趋势一：区块链已从探索阶段进入应用阶段

2018 年 8 月，德勤公司发布了一份题为“2018 年全球区块链调查”的报告（如图 16.1 所示），指出区块链正处于转折点，正从“区块链测试”转向构建真实的业务应用。该报告对加拿大、中国、法国、德国、墨西哥、英国和美国 7 个国家、10 个行业年收入超过 5 亿美元的企业中的 1 000 多名熟悉区块链的高级管理人员进行访问调查。

其中，34% 的受访者表示他们的组织已经“正在生产”区块链项目，而另有 41% 的受访者预计 2019 年将部署区块链应用程序。

如图 16.2 所示，近 40% 的受访者预计他们的组织 2019 年将在区块链技术上花费 500 万美元或更多。74% 的受访者已经参加或很可能会参加某个区块链联盟。

报告显示，越来越多的企业正在考虑或已经将业务系统与区块链结合，如图 16.3 所示，区块链正在金融、供应链、物联网等众多传统或新型行业中得到应用。

德勤报告中指出，虽然新技术企业采用区块链更为常见，但这一变化无疑表明区块链正在获得更广泛的认可，企业正在应用区块链，而非仅是探索。同时，区块链应用正在金融、供应链、公共部门等传统的行业成为设想或已经有实际使用案例。

除此之外，科技巨头们纷纷加大对区块链应用落地的布局力度，从商业应用辐射到 IoT 设备。IBM、Intel 等传统科技企业通过 Hyperledger 区块链联盟不断扩大在区块链领域的影响力



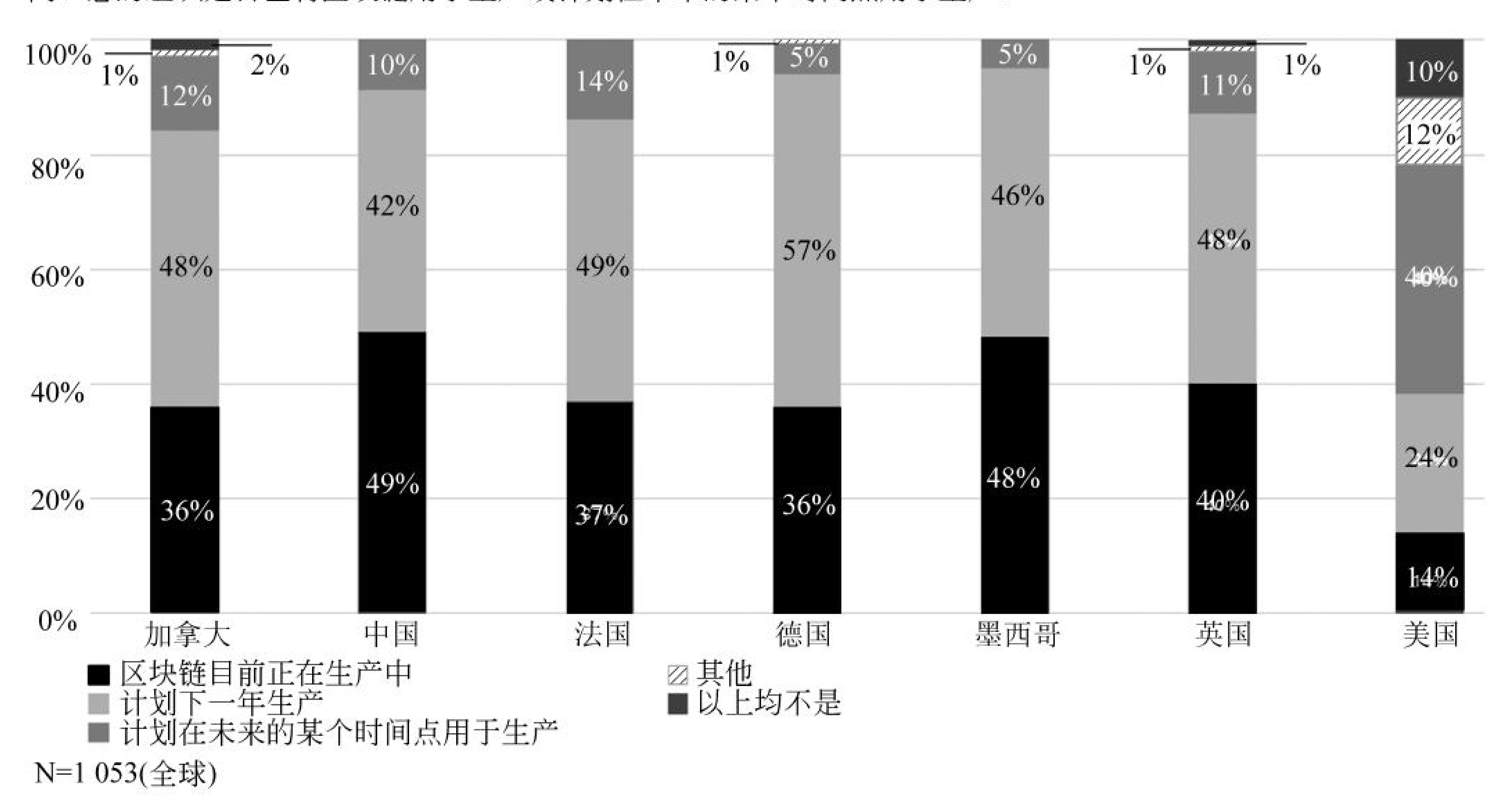


图 16.1　2018 年全球区块链调查（一）

资料来源：Deloitte（德勤）《2018 年全球区块链调查报告》

问：在区块链领域，您的组织明年将会投入多大的投资规模？

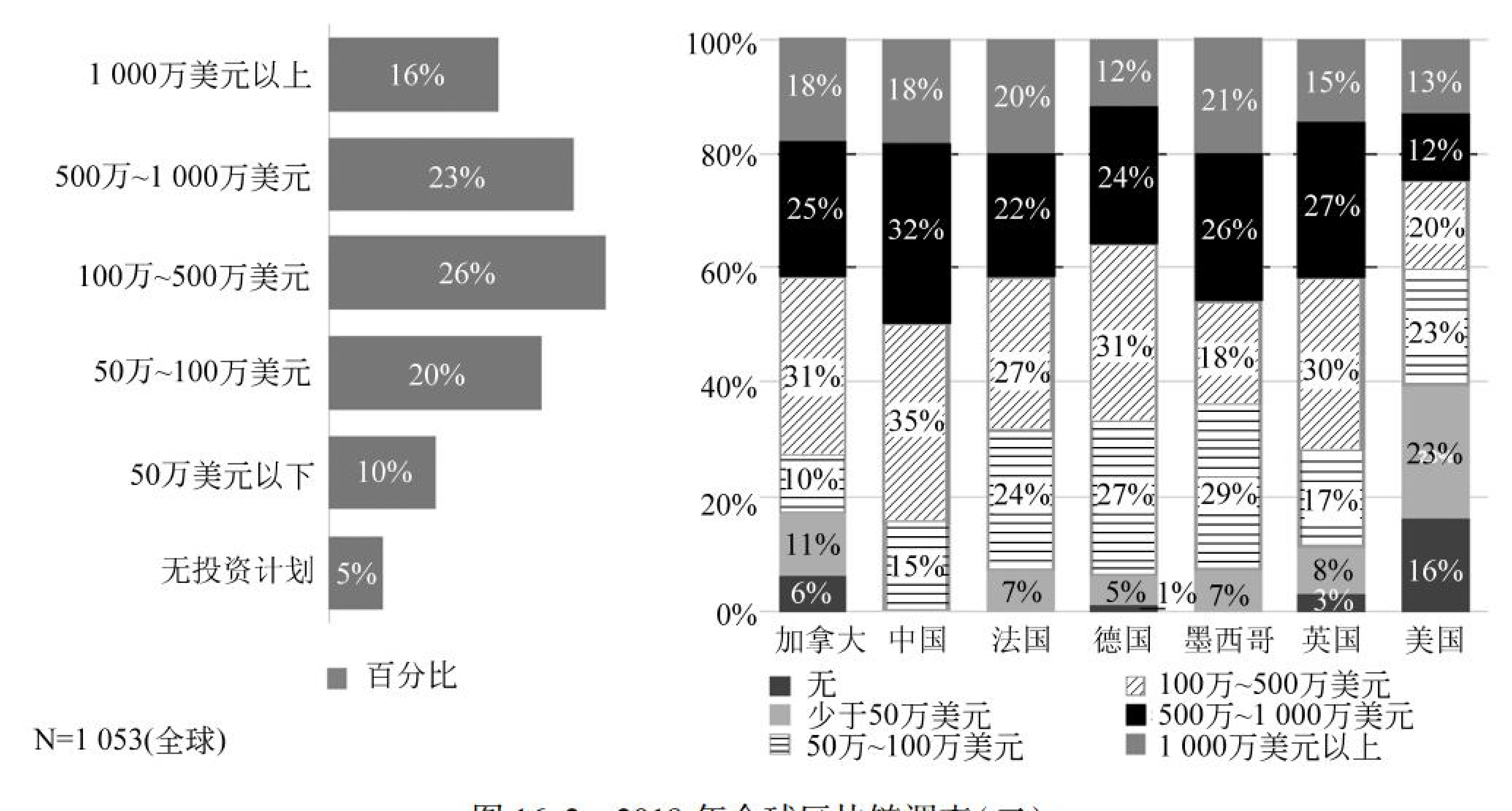
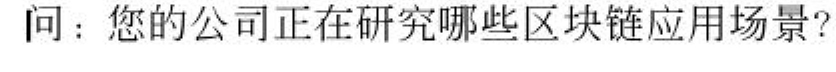


图 16.2　2018 年全球区块链调查（二）

资料来源：Deloitte（德勤）《2018 年全球区块链调查报告》



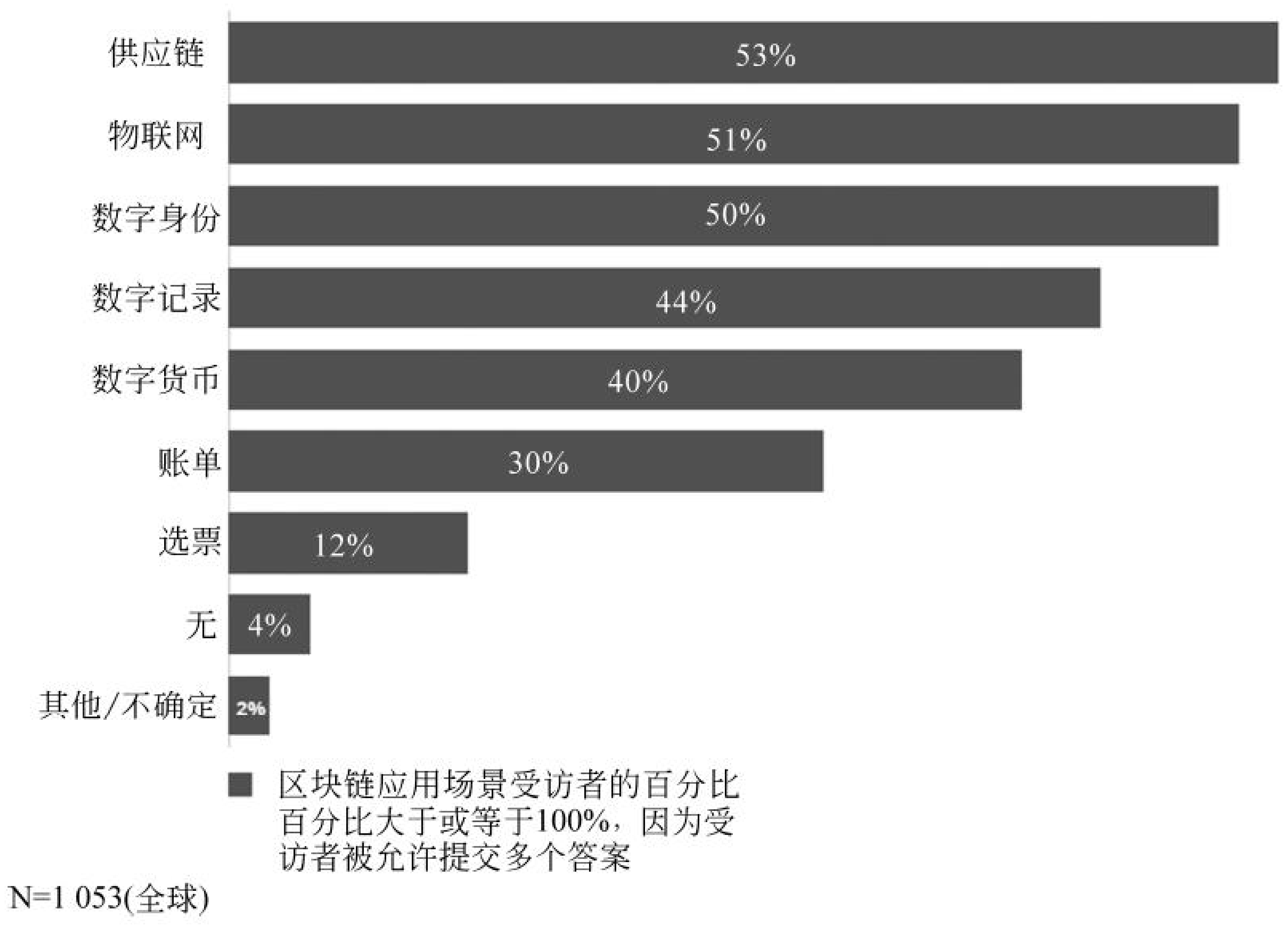


图 16.3　2018 年全球区块链调查(三)

资料来源：Deloitte(德勤)《2018 年全球区块链调查报告》

与应用范围。Microsoft 通过与以太坊合作提供了区块链服务平台，Amazon 在 AWS 上推出了区块链模板业务。

在国内，由工信部牵头成立的可信区块链联盟，吸纳了行业数以百计的单位参与，旨在推进区块链基础核心技术和行业应用落地(见图 16.4 所示)。华为、BAT 等行业巨头不仅发力


中华人民共和国工业和信息化部

Ministry of Industry and Information Technology of the People's Republic of China

搜索

工业和信息化部　新闻动态　信息公开　在线办事　公众参与　专题专栏　工信数据

首页 > 新闻动态 > 工作动态 > 司局动态 > 正文

信息化和软件服务业司参加可信区块链联盟成立大会

发布时间：2018-04-10　来源：信息化和软件服务业司

2018年4月9日，可信区块链联盟成立大会在北京举行。工业和信息化部信息化和软件服务业司巡视员李颖出席会议并致辞。中国通信标准化协会理事长奚国华、中国信息通信研究院院长刘多以及来自区块链领域的专家学者、知名企业代表等100余人参加了本次会议。

图 16.4　工信部牵头成立可信区块链联盟

资料来源：工业和信息化部官网

区块链服务平台，而且还在税务、金融、供应链、通信等诸多领域，积极引导并参与区块链与行业业务的融合与落地。

16.2　趋势二：企业应用成为区块链的主战场

区块链起源于比特币，并随着以比特币为代表的加密数字货币兴起而家喻户晓。然而，伴随着加密数字货币泡沫的逐步消退，人们愈发清醒地认识到，比特币等加密数字货币并不等于区块链。区块链自身的去中心化、多方协同、防篡改等技术特征所发挥的作用逐渐凸显出来，成为企业关注的重点。以数字货币为核心的公有链无论在效率方面，还是在扩展性上，均远远无法满足真正的企业业务的需求。与之相对应的，面向企业应用的联盟链、私有链，正逐渐成为区块链蓬勃发展的中坚力量。

以 Hyperledger 为代表的区块链联盟，参与企业成员已超过 250 家（截至 2018 年 8 月），其面向企业提供联盟链、私有链的核心技术，被众多科技巨头利用，正在向数以百计的企业提供区块链应用服务，服务客户遍布政府、金融、能源、供应商等多个领域。

而区块链的另一巨头以太坊，则联合了多个领域 300 余家企业（启动成员如图 16.5 所示，包括微软、英特尔、摩根大通等），正在雄心勃勃地推进企业级以太坊联盟（Enterprise Ethereum Alliance）的建立，旨在通过联盟链/私有链技术，降低企业成本，实现成员间的高效互通。

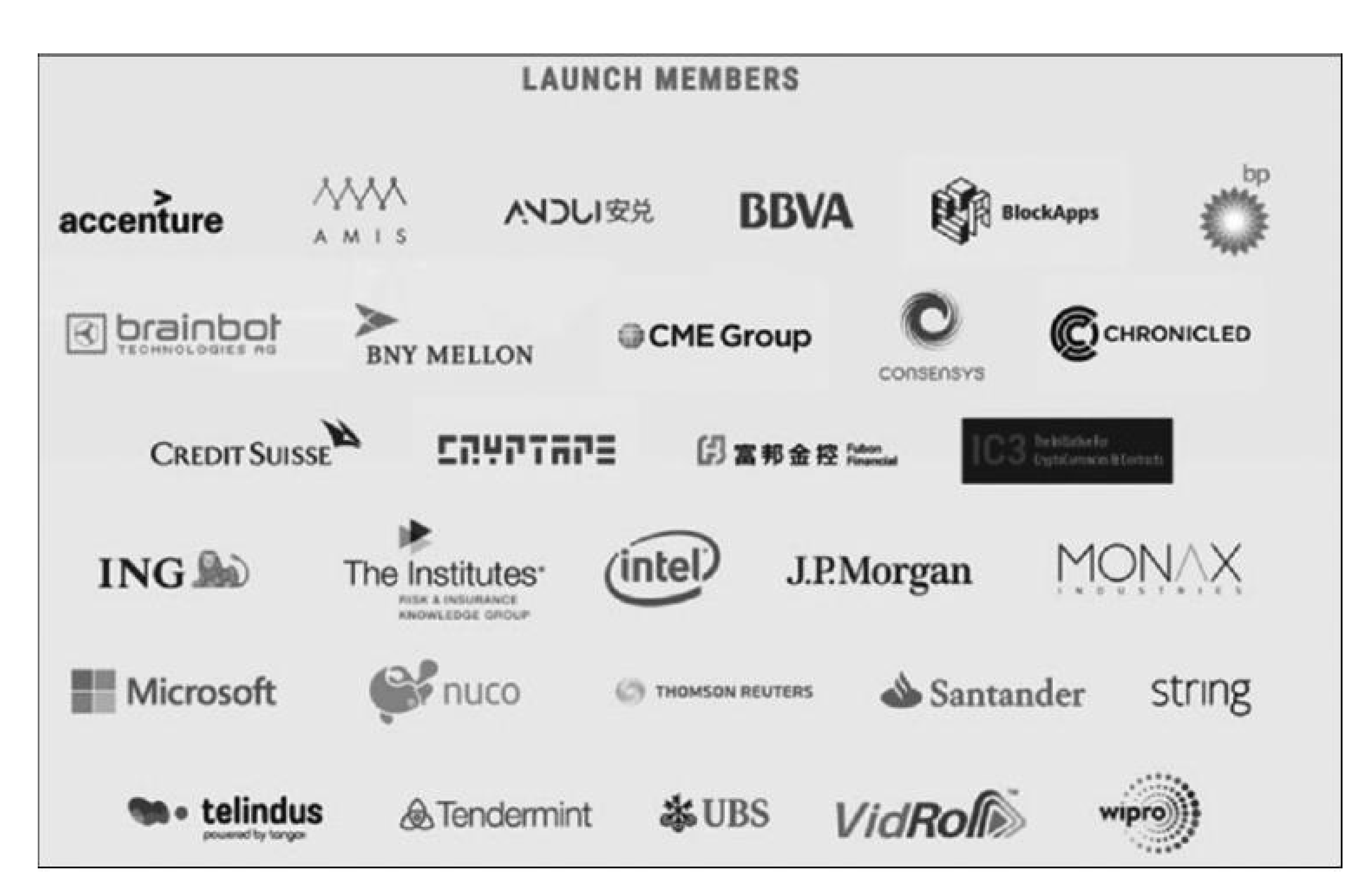


图 16.5　以太坊联盟

资料来源：企业级以太坊联盟官网

因此，我们可以看到，随着区块链技术的逐步发展，企业应用正在成为区块链发展的主战场，而企业应用与区块链技术的深度结合，也成为区块链未来发展的一个必然趋势。

16.3　趋势三：区块链将是一种改变商业模式的基础设施

我们正面临着区块链和去中心化技术带来的一场新的技术革命。正如被誉为“数字经济之父”、《区块链革命》的作者Don Tapscott讲到的：“区块链代表着互联网的第二个时代，它将深刻改变行业。”

在信息互联网时代，人们通过互联网传递信息，互联网公司通过重新组织信息创造价值（比如广告竞价排名、电商商品推荐等）。与此同时，这些具有中介性质的行业巨头位于网络顶端，承担着信任的创造与维护工作，并形成了一个互联网垄断时代。

然而在互联网的第二个时代，人们更多地希望通过互联网传递价值（例如：金钱、股票、身份信息等），然而价值传递的核心是信任，人们希望信任不再由这些强大的中介机构创造，而是通过一种共同参与的、公平可见的、安全的机制和技术完成。区块链使得信任的创造不再依赖于某一个组织或者机构，而是成为一种通过技术手段、共同协作完成的共识结果。无论是政务领域的区块链发票，还是金融领域的区块链跨境汇款，区块链技术的引入，使得信息传递不再仅仅是一组记录数据的拷贝，而是一种经过多方共识认可、具备法律效应、能够具体量化的价值体现。在ICT基础设施领域，区块链技术潜在地改变着CDN的生态，重构着漫游清算模式。可以说，区块链让互联网传递的不再只是信息，而是可以信任的价值。

基于区块链的价值互联网，正在以前所未有的速度扩展并影响着我们的生活，并且与互联网通信技术越来越紧密地耦合在一起，改变着当前的商业模式。未来随着价值互联网的不断发展，区块链无疑将成为承担价值交换的基础网络设施，而与之伴随的，是基于价值的可编程社会或将成为现实。

16.4　趋势四：区块链技术体系逐渐清晰，应用正在加速落地

中国信息通信研究院发布的《区块链白皮书》指出，近年来随着区块链技术的发展，区块链技术体系正逐渐清晰。各区块链平台在具体实现上虽然有所不同，但是在架构方面存在一定的共性，均包括共识、账本、智能合约等关键技术，各项关键技术不断向前演化。《区块链白皮书》中还提到，联盟链是区块链现阶段重要的落地方式，未来公有链和联盟链的架构模式将开始融合，并出现公有链与联盟链互相结合的混合架构模式，并利用钱包等入口，形成一种新的技术生态。同时，区块链服务以云计算平台为依托，使开发者可以专注于将区块链技术应用到不同的业务场景，帮助用户更低门槛、更高效地构建区块链服务，为企业、政府等客户创造全新的产品和商业模式。

随着区块链技术的革新升级，与云计算、大数据、人工智能等前沿技术的深度融合与集成创新，其技术体系架构逐步走向成熟，区块链将服务于金融、司法、工业、媒体、游戏等多个领域的商业应用，服务于实体经济和数字经济社会建设。

未来,随着区块链应用场景的日趋复杂,区块链与各个产业结合的日益紧密,跨链协同、线上线下交互、安全与数据隐私保护等区块链相关技术的重要性不断增强,将为区块链的技术体系带来新的机遇与挑战。

16.5 趋势五:区块链知识产权保护的竞争愈发激烈

随着参与区块链技术的企业逐渐增多,各主体间的竞争将会越来越激烈,竞争的范围也将不断扩大,企业对于区块链的技术、产品、商业模式等的需求,将会逐步扩展到对区块链相关专利的竞争与保护,未来企业将在专利保护方面加强布局。

当前,各大公司和组织机构已经开始纷纷加码知识产权竞争,力图在区块链竞争中跑马圈地。在全球领先的知识产权专业媒体 IPRdaily 正式对外发布的"2018 年全球区块链专利企业排行榜"显示,区块链专利技术数量进入快速增长阶段。从地域角度来看,目前区块链专利主要分布在北美洲的美国、欧洲的英国、亚洲的中国和韩国,以中国和美国最为突出,中美两国企业在区块链专利的申请数量上,几乎各占半壁江山。从行业角度看,中国的互联网巨头百度、阿里巴巴、腾讯,通信巨头华为等高科技公司悉数入榜,金融领域的巨头中国人民银行、Bank of America 也出现在榜单中,能源领域的中国国家电网、大众消费领域的沃尔玛等机构也纷纷登上榜单。

可以预见,未来区块链专利申请仍然以企业为主导,专利争夺将不断加剧,内容涵盖的范围将遍布金融、供应链等众多应用领域,呈现多元化态势,区块链知识产权保护的竞争将愈演愈烈。

16.6 趋势六:区块链标准规范的重要性日趋凸显

当前区块链项目日益增多,项目的质量与标准差别很大、良莠不齐,难以形成统一的规范体系,导致区块链项目兴起快、消亡也快。因此,亟待形成一套规范的标准体系,用于指导区块链技术与监管的规范工作,降低区块链技术与产品、产业之间的衔接成本。

全球区块链标准制定权已经在激烈的争夺之中,美国、欧洲国家和亚太区国家纷纷发力,中国也在积极参与。2016 年 7 月,工信部信息化和软件服务业司印发了《关于组织开展区块链技术和应用发展趋势研究的函》(工信软函[2016]840 号),委托工信部电子标准院联合多家国内重点企业开展区块链技术和应用发展趋势研究工作。2016 年 8 月,工信部电子标准院在北京组织召开了区块链技术和产业发展论坛筹备会暨白皮书编写启动会,对我国区块链技术和应用面临的机遇和挑战进行了讨论。2016 年 10 月,工信部发布《中国区块链技术和应用发展白皮书》,书中分析了国内外区块链发展现状及典型的应用场景,提出了描绘我国区块链技术发展路线图的建议,并首次提出构建区块链标准体系框架的建议,如图 16.6 所示。

2018 年 6 月,工信部公布《全国区块链和分布式记账技术标准化技术委员会筹建方案公

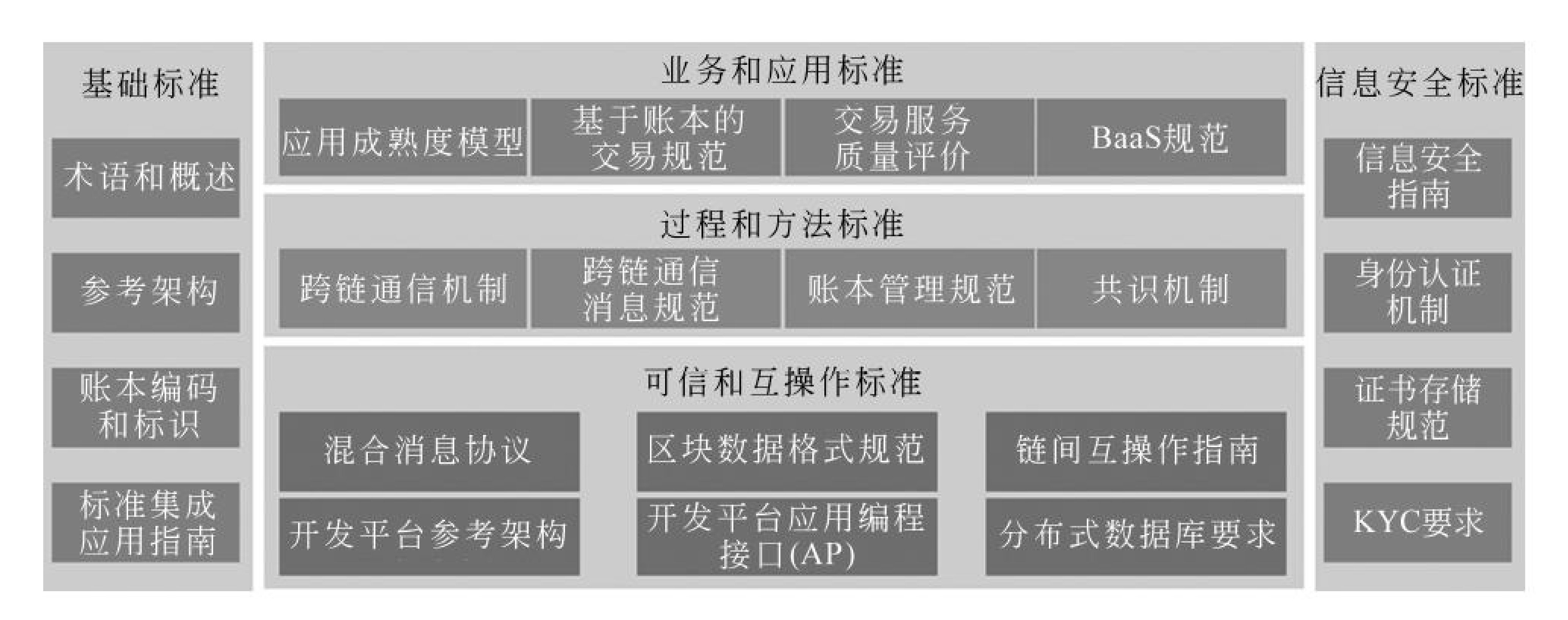


图 16.6　区块链标准体系框架

资料来源:《中国区块链技术和应用发展白皮书》

示》,提出了基础、业务和应用、过程和方法、可信和互操作、信息安全 5 类标准,并初步明确了 21 个标准化重点方向和未来一段时间内的标准化方案。

未来,区块链的标准将结合各个产业的需求,以凸显区块链价值为导向,围绕扶持政策、技术攻关、平台建设、应用示范等多个层次与维度,不断规范区块链的技术体系和治理能力,指导区块链相关产业发展。

16.7　趋势七:区块链和新技术结合带来新的产品与服务

区块链的影响力,不局限于区块链自身的技术领域和相关的产业生态圈,它还不断与云计算、大数据、人工智能等最火热的新技术结合,碰撞出新的火花。

在与云计算结合方面,各大云厂商们将区块链技术与云服务深度结合,将区块链作为云的重量级服务。国外的亚马逊 AWS 云服务平台、微软 Azure 云平台等均推出了区块链服务产品, 国内的华为、百度、阿里巴巴、腾讯等高科技巨头企业,同样将区块链技术与云结合,推出多款“云 + 区块链”的产品及解决方案,满足各领域企业对于区块链服务的诉求。

在与大数据结合方面,区块链的可信任性、安全性和不可篡改性,保证了数据的质量,并打破了信息孤岛的障碍,增强了数据间的流动。区块链新的分布式账本数据存储方式,也在影响着传统数据库和存储系统等大数据基础技术的形态。星际文件系统 IPFS,基于区块链技术实现了一种去中心化的分布式存储与访问方式,降低了异构数据的存储成本。BigchainDB 利用区块链技术实现了一种去中心化的数据库系统,使数据真正被掌握在用户手中。亚马逊公司基于区块链的技术特点,推出了一款新的量子账本数据库 QLDB,实现了对数据更改历史的准确记录与追踪。

在与人工智能结合方面,区块链重构生产关系,人工智能可以提高生产力,二者优势互补,具有很大的应用潜力。部分公司正在尝试通过区块链构建去中心化的机器学习系统,从

而达到构建安全可信、能够保护用户数据隐私性的高效机器学习平台的目的;另外,也有公司在尝试通过区块链构建机器学习模型和算力的交易平台,使得机器学习从业者可以通过这些平台进行模型和算力的共享。

16.8 本章小结

本章作为本书正文的最后一章,对区块链技术的发展趋势进行了前瞻性的展望。随着区块链技术的不断发展,区块链已逐渐进入应用阶段,而企业应用将成为区块链下一步的主战场。或许,区块链最终会像互联网一样,成为一种基础设施。研究调查也显示,区块链技术在各个领域应用的落地将越来越迅速。由于区块链还处于前期发展阶段,知识产权布局和保护显得尤为重要,各大机构都在争相抢占。区块链作为一种基础设施,制定标准规范也成为各大机构竞争的重要方向。至此,相信读者通过本书已经对区块链有了全方位、多层次的了解和感悟。

附录一
区块链常见问题解答

1. 什么是硬分叉和软分叉?

由于区块链是一个链表结构,当把不同的新区块连接到同一个旧区块后就会出现分叉。一般来说,经过一段时间,由于不同的人选择不同的分叉出块,而且速度会有差异,这不同分叉的区块链长度就会有所不同。按照以比特币为代表的区块链的规则,一般是选择最长的分叉作为主链而舍弃其他较短的分叉,这时分叉便会被消除了。

但如果有一部分人坚持选择某一条较短的分叉,这时就会与主链分道扬镳,成为了两个不同的区块链系统。这时我们就说,这个新的区块链系统是从原有的系统中硬分叉出来的。如果区块链系统出现比较大的升级,一般也会进行硬分叉,一部分矿工会用新的规则挖矿,另一部分会遵循旧的规则。最后的结果,要么是旧的矿工逐渐放弃旧规则,要么继续分叉出现两个系统。例如,比特币和比特现金,以及 ETH 和 ETC 均是硬分叉的产物。

所以我们看到,通过硬分叉实现的升级是不向前兼容的,而如果这个升级是向前兼容的,即新的规则可以接受旧的规则下产生的区块,此时称为软分叉。

2. 量子计算机会不会对区块链造成威胁?

量子计算机是一种运用量子力学的特性使得计算机完成传统的电子计算机无法完成的算法的计算机。它在某些算法上的性能远远超过传统计算机,比如大数分解算法。传统计算机分解一个大数的复杂度是呈指数级增长的,而量子计算机只需要多项式时间复杂度。现在主流的 RSA 加密算法就是基于大数分解的指数复杂度保证安全的,显然,在量子计算机面前

RSA 加密算法将不再安全。虽然现在量子计算机还处于研究阶段,但在不远的将来,量子计算机实现商用是可以预见的。

因此,有可能发现一种算法使得量子计算机能够以极高的效率运算 SHA-256 哈希值,这无疑对那些运用 PoW 共识算法的区块链项目产生威胁。它还可能破解椭圆曲线算法,从根本上破解区块链的安全性。然而,先不说量子计算机到底能不能真的破解这些算法,就算真的可以,对于区块链来说也没什么必要太担心。人们必然还能发明出许多量子计算机破解不了的密码学算法,到时候只需要进行一次算法升级的硬分叉,区块链网络还是可以正常运行。

3. 区块链对于链上资产的描述、记录能力是怎样的?支持哪些类型的资产?资产的生命周期怎么管理?

早期像比特币这样的项目仅能记录对应加密数字货币的交易历史,现在主流的区块链系统都是通过智能合约来承载资产,用户可以自由定义自己的资产。合约中的资产可以理解为一个会被持久存储的变量,变量类型可以是一个复杂的结构,所以可以描述丰富的信息。至于资产类型以及生命周期管理均由智能合约编写者来决定,这个是开放给智能合约编写者的。

4. 链上交易记录的内容,可以包括哪些信息?

链上交易记录的内容同样取决于智能合约是怎么编写的。一笔交易可以记录很多信息,信息的多少取决于智能合约的用途,比如,可以做转账、投票、存证等。

5. 谁负责记账?记账节点有多少个?节点的所有者是谁?

区块链是一个复式记账的模型,所有的记账节点都会记录同一本账,记账节点数量没有限制,节点间依靠 P2P 网络实现最终一致性。

通常在公链里(比如比特币、以太坊),每个节点对应一对公私钥,谁拥有这对公私钥谁拥有该节点。一个组织或个人也可能拥有很多节点,各个组织自行治理自己的节点,组织之间互相同步、互相鉴别数据。

6. 作为非专业人员如何使用区块链?

很多非开发人员提到区块链的时候,一般指的是加密数字货币,他们与区块链会产生的交集一般也是买卖加密数字货币。拥有以太币等加密数字货币可以参与以太坊等平台上面的许多 DApp 项目。如果非专业的开发人员想使用区块链技术,那么根据不同情境会有不同的选择。如果个人想要开发一些简单的区块链应用,可以选择以太坊等支持智能合约的公有链,这些大型的公有链一般都有很详细的教程。如果是小型组织想要发行自己的代币,同样可以学习使用以太坊上面的智能合约。如果企业用户想要通过区块链技术来创造一些更为通用的区块链应用,不再受限于与公有链绑定的加密数字货币的束缚,那么,可以选择一些企业级的区块链平台,比如 Quorum、Corda 以及华为 BCS 等。

其中,华为 BCS 是面向企业及开发者的高性能、高可用和高安全的区块链技术平台服务,

可以帮助企业和开发人员在华为云上快速、低成本的创建、部署和管理区块链应用。

7. 联盟链相比公有链是否失去了去中心化的特性?

在区块链技术发展的最初阶段,区块链和“去中心化”是绑定在一起的,人们认为去中心化是区块链的最大特点。然而近年来,随着区块链技术的发展和人们对于区块链理解的深入,人们发现区块链的许多特性并不需要完全地去中心化。适当地降低去中心化程度可以提高共识效率,或者更加适配特定的应用场景。联盟链就是对这种思想的有效实践。联盟链中的各个节点都是经过审批加入的,所以可以放宽它们的权限来提高效率。从这种意义上讲,联盟链确实不够去中心化,只能说是“弱中心化”或“多中心化”。但实际上,这并没有减少其作为区块链的种种特性,比如可追溯性、不可篡改性等。

8. 区块链是不是“割韭菜”的工具?

“割韭菜”常用于股票市场,指的是大型机构通过提高股价、吸引大量散户买入股票,然后在股价达到高点的时候卖出股票,将散户的钱收入囊中的做法。加密数字货币的交易市场出现以后,由于加密数字货币的资本基数小、加入门槛低、监管不完善等特点,使得“割韭菜”在加密数字货币领域远远比股市容易。金融机构们必然不会眼睁睁地放弃。所以,在虚拟货币市场泡沫巨大以及 ICO 比较疯狂的时期,区块链的确被当作“割韭菜”的工具。正如枪炮可以杀人,亦可保家卫国,区块链在有些人手里是骗钱的工具,在有些人手里是变革社会的武器。从另外角度来讲,那些被割的“韭菜”通常是那些盲目跟风、不理性、贪婪、妄图一夜暴富的人,而那些谨慎理性的投资者则不会轻易地被割。可见,他们遭受的损失,根源并非区块链。

9. 区块链是不是分布式数据库?

区块链最重要的特点就是每个节点都储存一份完整的账本,很多人都管区块链叫分布式账本,所以它是不是就是一个分布式的数据库呢?区块链储存交易信息的确是运用某种数据库结构(比如 LevelDB、SQLite 等),而且它的节点又的确是分布式的。但是当我们把这两个词合起来的时候,分布式数据库在现实工程中是有特定的特性和要求的。分布式数据库和区块链的共同点不再赘述,它们的区别点还是有很多的。首先,区块链是去中心化的分布式系统,而分布式数据库则具有明显的中心化特征。进而,区块链需要处理由去中心化而带来的拜占庭将军问题,而分布式数据库则无需关心拜占庭将军问题。其次,区块链不单单如分布式数据库一般只是负责承载数据本身,而是通常需要与智能合约结合起来作为一个功能完整的应用,可以处理复杂的业务逻辑。其他还有一些区别点,诸如:分布式数据库有管理员权限,有单一管理入口,区块链所有节点都可按需配置权限,存在多个管理入口;数据库可以删除历史内容,区块链不可以删除历史内容等。区别还有很多,不再一一列举。

10. 加密数字货币真的有价值吗?

货币的本质是一般等价物。我们传统意义上的货币之所以有价值是因为大家都认可它

有价值,大家都愿意用实际的商品与它作交换。面包有吃的内在价值,车有出行的内在价值,而纸币只不过是一张纸,黄金只不过是一块金属而已。由于比特币和黄金一样具有稀缺性、防伪性、可分割性等特点,可以被用作一般等价物。从当年 10 000 比特币购买了两个比萨开始,比特币就已经可以用来买东西了。如今,比特币、以太币、门罗币等加密数字货币都可以用来购买商品,而其他加密数字货币在一些交易所也可以交换成法定货币,因此可以认为它现在是有价值的。法定货币也可以变得没有价值,同样的,当人们对于某个加密数字货币失去信任的时候,它的价值也会随之消失。

2013 年 12 月,中国人民银行等五部委发布了《关于防范比特币风险的通知》,发文中明确定义比特币是一种特定的虚拟商品,不具有与货币等同的法律地位,不能作为货币在市场上流通使用。可见,加密数字货币在某种意义上确实存在价值,但其并非法律认可的货币。

11. 加密数字货币的转账是匿名的吗?

区块链的账户本质上是一个公私钥对,不需要和现实身份挂钩,从这个意义上讲它是匿名的。不法分子利用比特币来洗钱,或者在暗网上做非法交易。但不能说它是完全匿名的,因为每个人手里都有一份完整的账本,所有的交易都是公开可查的。如果将区块链的账户和现实身份对应起来就会暴露这个人的交易历史。有一些加密数字货币专门为此创造了解决方案,比如门罗币、达世币、Zcash 等。这些加密数字货币用一些加密算法使得转账记录可以被验证但不可被浏览,所以可以实现匿名。

12. Hyperledger Fabric 系统中,用户在区块链上的账户是什么样的,账户信息可以包括哪些?

区块链上的账户是用智能合约来承载的,所以,Hyperledger Fabric 系统中的账户均由智能合约来定义,可以由智能合约中的多种数据结构来存储;账户可以包含丰富的信息,我们可以创建一个复杂结构来承载丰富的信息,因此技术上可以包括现有系统的各类信息,如用户名、账户创建时间、地址信息、余额、历史交易等。

13. 区块链和去中介的关系是什么?

由于区块链网络没有一个中心节点,所有的价值交换都是点对点进行的,不需要第三方中介的认证或背书,所以很多人将区块链视为一种去中介化的工具。而金融领域的主要工作是资产权益的发放和流通,比如股票和债券的发行和交易。从这个角度来看,大型金融机构的主要角色其实是中介。那么,区块链是否能够能够取代这些作为中介的金融机构呢?这里我们可以看一下 ATM 机的例子。ATM 机发明之前,银行柜员每天绝大部分的工作就是存钱和取钱。后来,绝大多数的存取款工作被 ATM 机代替,银行柜员的职位并没有消失,他们有更多的时间来处理存取款以外的业务,工作效率大大提高。区块链对于中介的作用其实也是类似的,它不会完全取代中介,而是解放中介的生产力,提高中介的效率。比如金融业务的三大流程:资产权益的评估、资产权益证明的发放和资产权益证明的流通,其中评估这个过程是

无法以区块链代替的,而权益证明可以用区块链的 Token 来代替,但将其与实际价值物联系起来的仍然是中介机构。而区块链最显著的作用,是大大提高资产权益证明流通的效率。因此,区块链并不一定是完全去中介化的。

14. 加密数字货币和数字货币以及法定数字货币的关系是什么?

数字货币在很多情况下就是代指加密数字货币,但是也很容易想到数字货币的形式不止加密数字货币。但实际上,目前的电子支付中所交换的并不是真正意义上的数字“货币”,而是银行的资产证明,你只能通过银行才能把它换成法定货币。而真正意义上的数字货币必须是由央行发行的法定数字货币,这种数字货币无须由银行兑换,其本身就是法定货币。

加密数字货币是否可以称为“货币”众说纷纭,由于加密数字货币没有国家信用背书,很多专家认为只有法定货币才能被视为真正的货币。事实上,如今的比特币等少数几个加密数字货币已经被大量用作支付和购买商品,部分符合货币的价值尺度、流通手段、贮藏手段和支付手段四种职能。但正如问题 10 最后所述,目前在我国,加密数字货币并非法律上认可的币。

而加密数字货币之所以能够有这么良好的货币性质正是区块链技术所保证的。所以人们会理所当然地认为法定数字货币就是央行发行的加密数字货币。但事实上,区块链对于法定数字货币的研究有一定的借鉴意义,但必须得结合具体的需求来选择具体的技术。因此,加密数字货币是法定数字货币的重要参考,但不是必然的形式。

15. 区块链技术都很耗电吗?

谈及区块链技术,很多人都会将其与高能耗联想到一起,正如第一章所介绍的,比特币对能源的消耗程度已经达到了可以用“恐怖”一词来形容的地步。然而,区块链并不等于比特币,当前的区块链系统从公有链、联盟链到私有链不一而足,而不同的区块链系统,其能耗情况其实也千差万别。比如以 Hyperledger Fabric 为代表的联盟链系统是可以运行在通用服务器上的,并不需要高能耗的矿机来进行共识。所以,说区块链技术都很耗电是片面的。

16. 区块链不可篡改是指不可以做任何修改了吗?

“修改”可以从两个方面来解读:其一是对当前数据的增量修改;其二是对历史数据的直接修改。针对前者,区块链保证账本历史的不可篡改性,即账本数据的历史变动踪迹是不可修改的,但仍然支持对当前数据按照智能合约提供的接口进行增量修改。而后者才与区块链的不可篡改特性直接相关。区块链的不可篡改特性是区块链最基本的优秀特性之一,然而不可篡改也并不意味着在任何时候都可不修改。

区块链的不可篡改特性是区块链最基本的优秀特性之一,然而不可篡改并不意味着在任何时候都不可修改。首先,可以将区块链系统所使用的共识算法分为强一致共识和弱一致共识。针对强一致共识(如 PBFT),一旦某一个区块通过了共识过程,那么这个区块就是确定了

的，不可篡改。而针对弱一致共识（如 PoW），虽然某一时刻已经产生了一个区块，但是这个区块仍有可能在后续共识过程中由于全网的主链选择而被抛弃，也就是"分叉"过程。而更特别的，以 PoW 为例甚至会受到 51% 算力攻击的威胁，也就是说，一旦某一方掌握了超过 51% 的算力，他可以在系统里为所欲为，任意修改。所以，针对弱一致共识，通常需要更长的时间来保证某一笔交易被确认的概率，如比特币需要再生成 6 个区块才能在很大概率上保证当前区块不会被篡改，但仍然不能免于 51% 算力攻击（虽然这极难做到）。另外，不可篡改是说我们不能修改所有节点的数据，但我们依然可以修改本地节点的数据，只不过尽管我们可以修改自己的数据，但是其他未被修改的节点不会相信我们修改了的数据，我们"自欺欺人"其实是无效的。所以，我们需要辩证地来看待"不可篡改"这一特性。

17. 区块链可监管吗？

区块链系统的可监管性需要结合具体情况来看。公有链系统对所有参与方都是交易透明的，但是其隐私特性一定程度上为监管带来了不便。而联盟链和私有链则加入了准入机制和权限控制的特性，这为监管带来了极大的便利，我们可以通过加入监管方，并为监管方设置一定查询权限达到监管目的。

18. 区块链系统的"不可能三角"是指什么？

区块链系统的"不可能三角"是指衡量区块链系统的三个指标不可能同时达到最优，这三个指标分别指：可扩展性、安全性和去中心化程度。可扩展性其实包含了两个方面的含义：一是系统性能表现良好（吞吐量高，交易确认时延短）；二是指系统需要支持节点扩展能力，并且节点扩展时系统整体性能不会下降。安全性是指区块链系统要保障整体安全可靠，在一定假设条件下系统不会被攻破。去中心化程度就是指整个系统是不是去中心化的，是否存在具有一些特权的特殊节点等。虽然，"不可能三角"并不像分布式系统里的 FLP 或者是 CAP 定理一样有着严格的证明，但是目前的区块链系统确实只能在这三个指标中的两个里表现优秀。

19. 区块链技术当前面临什么挑战？

区块链技术当前所面临的主要挑战包括：处理交易的性能需要持续提升，用户隐私需要进一步保护，应用场景需要进一步拓展等。华为区块链服务（BCS）在面对这些挑战时均做了一定有意义的工作：针对处理交易的性能，BCS 现已达到单通道 5000 + tps 的吞吐量水平，处于业界领先水平；针对用户隐私保护能力，BCS 正在积极构建基于零知识证明和同态加密的解决方案；而针对应用场景，BCS 一直在积极寻求各行各业的合作伙伴，期待可以打造"爆款"应用，尤其希望能够结合区块链技术产生模式创新的应用，充分利用区块链技术的几大特性，发挥区块链的最大价值，进而助力区块链被更多的人所认知，吸引更多优秀人才进入区块链领域，推动区块链技术本身的发展。

20. 中本聪身份之谜

2008 年 10 月 31 日，一个化名为中本聪（Satoshi Nakamoto）的神秘人（或神秘组织）在一

个密码学邮件列表中发表了比特币白皮书。2009 年 1 月 3 日,中本聪开发出比特币的程序并挖出了创世区块,获得了 50 个比特币。这个开创了区块链时代的天才,其身份却一直都是一个谜团。他在 P2P Foundation 网站的个人资料里自称是一名日本人,且跟外界交流只通过邮件列表的形式。但他从来没有用日语进行过任何交流,而且他的英语之流利程度与英语母语者无异。他常常切换英式英语和美式英语,而且在一天中选择随机的时间来发送邮件,让人无法猜测他所在的时区。他在该密码学邮件列表中地位非常显赫,而该列表中的成员不乏密码学界的大师。后来他将比特币的官网 bitcoin. org 交由其他人掌管,并逐渐销声匿迹。

2010 年末,维基解密准备接受比特币捐款,此时中本聪突然发邮件表示不建议这样做,认为比特币尚不成熟。后来,中本聪便不再在邮件列表中露面。但中本聪的神秘引起了媒体的狂热兴趣,各种报道纷纷猜测中本聪的真实身份,媒体所报道的候选人越来越多。但后来被认为最有可能的,是美国《新闻周刊》在 2014 年 3 月 6 日所报道的 Dorian Nakamoto。他出生时的名字正是 Satoshi Nakamoto,且曾在军方从事保密性工作,另外还有很多其他的证据。但他本人极力否认自己是中本聪。就在报道当天,中本聪再次现身发文称自己不是 Dorian Nakamoto,这件事才逐渐平息下来。而后,中本聪再也没有出现过。2018 年 11 月 30 日,中本聪在 P2P Foundation 网站上的状态中添加了一个单词“nour”,并关注了一个密码圈的博主。由于该账号在 2014 年曾遭受过攻击,所以本次操作是否中本聪个人所为不得而知。

现在更多人则坚信中本聪并非一个人,而是一个团体组织,因为像比特币这种具有跨时代意义且设计如此精良的工作很难由一个人完成。还有人猜测中本聪匿名是为了躲避有关当局的追查,因为在 2007 年的时候,曾有数字货币 Liberty Dollar 和 e-Gold 被追查和对有关人员判刑。但后来加密数字货币大行其道的时候,出现了无数个其他加密数字货币的创始人,这些人都没有被抓,而中本聪也没有必要因为这个原因匿名了。但就有没有创始人而言,比特币相对于其他加密数字货币更能体现“去中心化”的思想,因为其他加密数字货币的创始人可能直接能够影响公众对该加密数字货币的信任程度,比如莱特币的创始人每次发 Twitter,或者卖出莱特币,都会或多或少影响到莱特币的价格。而比特币没有一个具体的人作为领袖,使得大家对它的信任更加放在这个货币本身。所以,中本聪的身份保持神秘对比特币也是具有重要意义的。

21. 智能合约到底“智能”吗?

这里首先要澄清一个概念,智能合约是“smart contract”,并不是“intelligent contract”,所以,智能合约本身并不包含类似人工智能中的“智能”概念。

智能合约其实是一个很早出现的概念,但直到区块链技术得到广泛认可,智能合约才在与区块链技术进行结合的前提下再次走进公众视野。然而,区块链技术的火热让很多人盲目地认为区块链可以解决任何事情,尤其是很多区块链系统支持图灵完备的智能合约开发环境,这让人们误以为智能合约达到了真正的智能。现实是智能合约依然要求我们在规则下做事,这里的规则是指智能合约开发环境所限定的规则(比如只能支持固定的操作码等),不是

我们用智能合约开发环境编写出来的规则。因此,我们在区块链系统上写智能合约依然是比较受限的,比如不能访问对不同节点呈现出随机特性的数据,不能访问不可信源的数据,不能访问系统资源等。不过,虽然智能合约开发环境是一个受限环境,但是我们依然可以写出很多完整、丰富的逻辑。所以,尽管“智能化”只是智能合约持续追求的目标,但当前智能合约只能说是在一定程度上达到了智能,但不能盲目乐观地认为智能合约可以完成我们需要的任何智能逻辑。

附录二

常见区块链产品及平台介绍

当前,区块链应用蓬勃发展,各类区块链平台层出不穷。尽管其中不乏许多盲目跟风且并无实际应用价值的“割韭菜”项目,撇去浮沫,仍有许多十分优秀的区块链项目和区块链平台值得了解和借鉴。本章将对部分主流的区块链项目及平台进行介绍,为读者提供一些参考。

一、比特币及其拓展

比特币的巨大成功带动了区块链的整体发展,然而,比特币区块链也存在着一些较为严重的问题,比如对计算资源有着极大浪费的 PoW 共识以及极为有限的脚本执行能力。因此,在比特币出现后,也有不少拓展项目及“山寨”项目紧随其后被推出,试图对比特币的一些缺陷进行弥补。本节将对比特币以及与其相关的几个项目进行介绍。

1. 比特币

正如本书前面章节所介绍的,比特币(见图 1)是一种去中心化的数字加密货币,它的设计思路在 2008 年由化名为“中本聪”的人或机构提出,并在 2009 年 1 月被正式发行。



图 1　比特币 logo

比特币的出现,可以说是对集中式货币政策、交易管理的挑战。通过比特币这样一个完全去中心化的加密数字货币,用户可以自由地进行交易,一方面跨越了现实世界中存在的许多壁垒,另一方面也给一些

非法交易提供了平台。然而随着比特币价值的不断上涨,逐渐出现了许多使用专用挖矿硬件、集中大量算力的“矿场”,这无疑削弱了比特币的去中心化特性。

比特币原生的区块链设计具有十足的开创性,引领了一系列区块链平台的产生和发展。然而,其本身由于节点完成工作量证明所需的大量计算对于资源的浪费以及随之带来的缓慢的交易确认时间以及低下的吞吐量,为区块链研究者所诟病。后续的许多区块链相关工作都是致力于改进比特币原生区块链的这些问题。尽管如此,比特币区块链系统仍是为数不多的(甚至可能是唯一的)从创建至今未发生过大规模的系统设计上的漏洞的区块链系统,其中的缘由还是很值得思考的。

比特币的官方网站是 https://bitcoin.org,其发展历程及主要大事件见图 2。

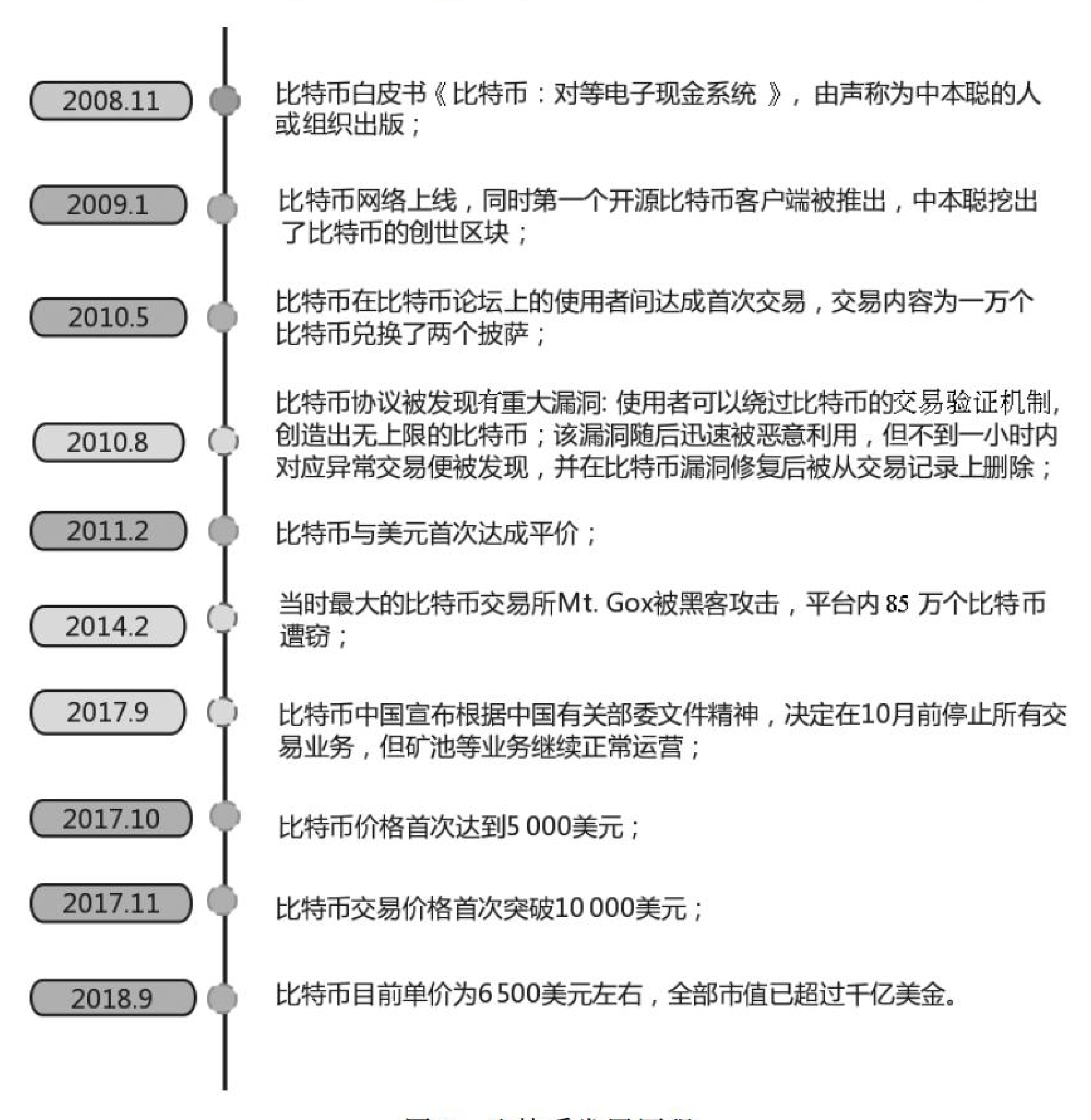


图 2　比特币发展历程

2. 闪电网络

随着比特币的不断发展,其缓慢的交易确认时间(等待 6 个块的可信确认大致需要一个小时)、远不能满足需求的交易吞吐量(每秒 7 笔左右)越来越不能满足急剧增长的交易需求。

首先引起比特币社区讨论的是比特币区块链的扩容问题。由于初始比特币区块链的单个区块体积有着 1MB 的限制，而逐渐增长的交易数目使得这部分空间逐渐被填满，因此需要对区块进行扩容。然而由于比特币区块链的去中心化特性，进行全球性的扩容并非易事。比特币社区针对这个问题提出了多种扩容方案，但至今仍没有达成关于何时扩容、扩容规模的一致意见。

2015 年 2 月被提出的闪电网络（Lightning Network）便起源于比特币扩容问题。简单来说，它通过将大量交易放置于比特币区块链之外进行，仅将关键环节放置于链上确认的方法，从另一个角度在一定程度上解决了比特币扩容问题。

闪电网络主要通过引入两种类型的交易合约：序列到期可撤销合约（Revocable Sequence Maturity Contract，RSMC）及哈希时间锁定合约（Hashed Timelock Contract，HTLC）。其中，RSMC 解决了链外交易通道中币单向流动的问题，HTLC 则解决了币跨节点传递的问题。两者结合，便构成了闪电网络，使得用户可以直接一对一进行交易，从而避免向整个区块链网络广播自己的业务，一方面能够在避免支付昂贵的交易费用的同时达到较快的交易速度，另一方面也可以对交易细节进行隐藏。

3. 侧链

侧链（Sidechain）概念上属于比特币区块链的一个拓展协议，该协议允许资产在比特币区块链与其他区块链之间流通。侧链主要是比特币区块链社区在面对众多“山寨币”以及以太坊等新兴区块链平台对比特币区块链的冲击时，为扩充比特币区块链底层协议而提出的。通过侧链，可以在不影响主链的主要功能的基础上，拓展交易隐私保护、智能合约等新功能。

简单来说，侧链可以是一个独立的区块链，即有自己的账本、底层的共识机制，可以支持各种交易类型、合约类型。侧链需要与比特币区块链挂钩来引入和流通一定数量的比特币作为自己的代币，当这部分比特币在侧链中流通时，主链上的比特币会被锁定，直到侧链比特币回流。类似闪电网络，侧链机制也可以将一些高频的交易放到比特币区块链之外进行，从而提高比特币区块链的吞吐量。

二、莱特币

莱特币（Litecoin，见图 3）是一种对等电子加密数字货币，用户可以以低廉的交易费向其他人进行付款或转账。莱特币从推出起便与比特币对标，在各个方面与比特币都十分相似。尽管如此，莱特币也有部分与比特币不同的设计，以期达到改进比特币的目的。两者的对比可以见表 1。



图 3　莱特币 logo

莱特币的总量是比特币的四倍，同时其每个币的出块时间是比特币的 1/4，从而使交易确认的时间相对更短；同时，莱特币也率先于比特币采取了隔离见证及闪电网络的拓展；共识协

表 1 比特币与莱特币对比

	比特币	莱特币		比特币	莱特币
货币总量	2 100	8 400	难度调整	每 2 016 个块	每 2 016 个块
加密算法	SHA-256	Scrypt	初始奖励	50btc	50ltc
出块时间	10 分钟	2.5 分钟	当前区块奖励	25btc	50ltc

议方面,莱特币使用了与比特币类似的工作量证明的机制。然而,为了削弱大规模矿池的影响,使莱特币更加“去中心化”,莱特币采用了不同的挖矿算法:用 Scrypt 代替了比特币使用的 SHA-256;这是由于在比特币原生的 SHA-256 挖矿算法下,挖矿的速度是与机器的算力成正比的,这就催生了专门的“挖矿专用集成电路”,即矿机。矿机的挖矿效率相比普通的 GPU 高数个数量级,从而导致算力越发集中于专用矿场,使得普通用户难以入场,降低了区块链的“去中心化”程度。而 Scrypt 是一种“内存难题算法”,其求解速度主要取决于计算机内存大小,因此 Scrypt 算法使得并行化的大规模矿场在莱特币中不再占优势,保证了莱特币的去中心化程度。

莱特币的官网为 https://litecoin.org,其发展历程及主要大事件见图 4 所示。

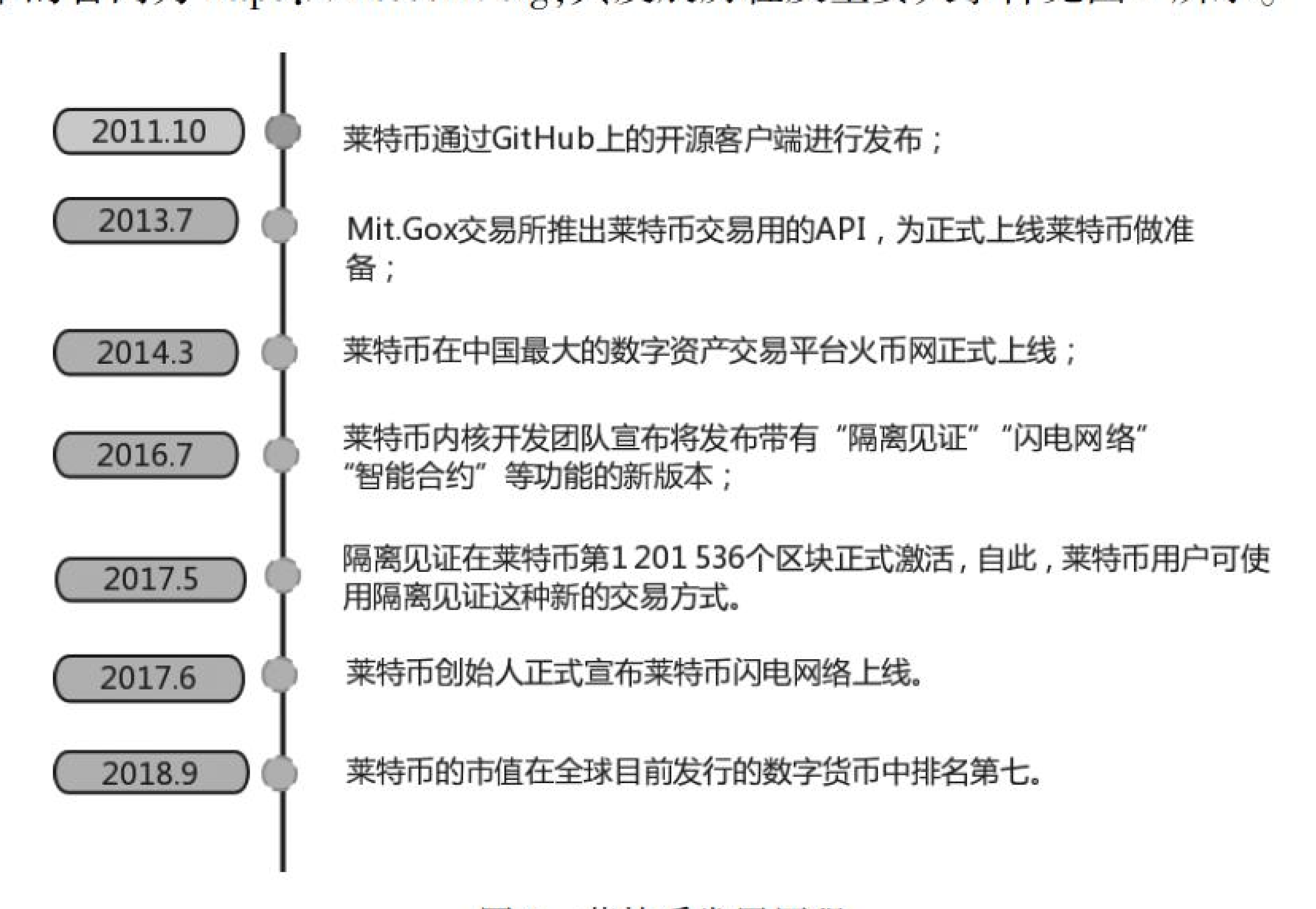


图 4 莱特币发展历程

三、以太坊

以太坊(见图 5)由 Vitalik Buterin 在 2013 年受比特币启发提出,并于 2015 年 7 月 30 日正式发布,其定位是“下一代加密数字货币与去中心化应用平台”。它是一个具有智能合约功能的公共区块链平台,是创造基于区块链的各种去中心化应用的基础。以太坊通过图灵完备的去



图 5 以太坊 logo

中心化虚拟机“以太坊虚拟机”(Ethereum Virtual Machine,EVM)来处理点对点合约。为了量化 EVM 执行操作的开销,防止某些恶意合约无限消耗以太坊系统计算力,以太坊引入了“汽油”(gas)的概念,即 EVM 处理点对点合约需要消耗“汽油”(gas),而汽油可以用以太币(Ether)进行购买。

以太坊的出块速度很快,基本维持在 15 秒出一个块的速率。这样相对来说较快(与网络同步时间相比)的出块速度会产生大量由于网络同步不及时而产生的未被收入到主链中的区块,即比特币中所谓“孤块”。在比特币系统中,由于出块速度被控制在 10 分钟一个块,相比于现有网络状况来说出块时延远大于传播时延,因此很少会出现孤块的情况,比特币系统便直接废弃掉这类区块。然而,以太坊允许主链上的区块头结构中包含对这些区块的引用,并称这些区块为“叔块”,挖出叔块的矿工也将会得到奖励,而挖出主区块的矿工也会因为包含叔块而得到额外的奖励。对叔块的引用进一步验证了其父块的有效性,增加了网络的安全性。对叔块的引用可以增加主区块的“重量”,在以太坊的共识机制中最重的链是主链。

相对于比特币小心翼翼尽量避免硬分叉(hard fork),以太坊的理念是大胆实验,遇到问题勇于使用硬分叉,其规划的不同版本就需要用硬分叉实现。2016 年 6 月,以太坊上的一个去中心化自治组织项目 The DAO 被黑客攻击,造成市值 5 000 万美元的以太币被转移。最后在 2016 年 7 月 20 日,以太坊进行硬分叉,做出一个向后不兼容的改变,让所有的以太币(包括被移动的)回归原处,但是有部分人不接受此改变,他们在没有更改的区块链上继续挖矿,成为以太坊经典(Ethereum Classic)。这是第一次有主流区块链为了补偿投资人,而通过分叉来更改交易纪录,引起了一定的争议。

以太坊的缺点在于,其应用代码本身及应用产生的数据都存在同一个区块链中,造成了区块链的快速膨胀,容易引起交易拥堵。目前以太坊正在研发不同的侧链(Sidechain)和离链(Off - Chain)技术以缓解主链的拥堵状况。此外,为了解决恶意合约造成节点无限循环执行,每个合约执行都有 gas 限制,导致它无法支撑大规模的应用。

以太坊目前采用的是工作量证明方式挖矿,采用的算法是 Ethash。该算法与莱特币使用的挖矿算法相似,都需要较大的内存,所以难以制造针对性的 ASIC 矿机,大众可以以相对不高的投入参与进来。在以太坊的规划中最后的阶段将会采用权益证明来对交易进行验证,即权益人通过缴纳一定数量的以太币作为保证金来参与验证工作,如果权益人做出不诚实的行为,其保证金会被罚掉。相较于工作量证明,权益证明可节省大量在挖矿时浪费的硬件与电力资源,并避免矿池引起的中心化。

以太坊的官网为 https://www.ethereum.org,其发展历程及主要大事件见图 6。

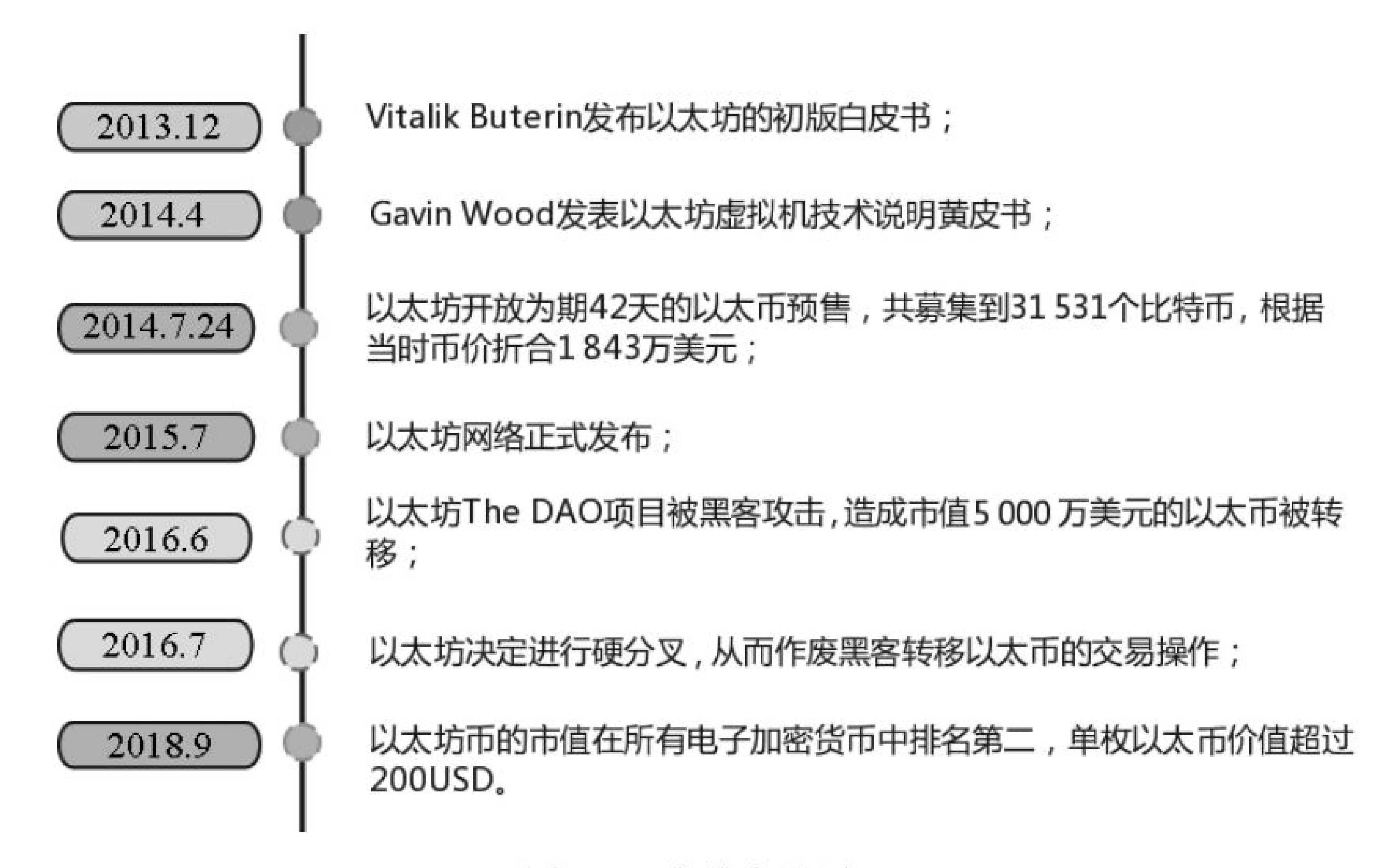


图 6　以太坊发展历程

四、EOS

EOS(Enterprise Operation System),是由 Block. one 团队主导研发的一个区块链操作系统。Block. one 的首席技术官 Daniel Larimer 是 Bitshares,Steem 和 EOS 的联合创始人。

EOS 可用于开发、托管及执行商用的分布式应用程序(DApp),它主要致力于解决现有区块链应用性能低、开发难度高、对手续费依赖较为严重的问题,从而实现分布式应用程序的规模性扩展,是“区块链 3.0”的代表性项目。

EOS 生态系统包括两个主要组件: EOS. IO 及 EOS 代币。其中,EOS. IO 在概念上等价于计算机的操作系统,它的主要作用是控制和管理整个区块链网络,并支持用户在其上进行分布式应用程序的开发和部署。EOS 代币则是 EOS 网络的加密数字货币。一个在 EOS 上进行分布式应用程序开发的用户需要持有一定的 EOS 代币,从而才能利用 EOS 网络的资源,但 EOS 本身并不对其上的应用收取手续费。同时,EOS 网络的用户也可以将自己持有的 EOS 代币所对应的资源分配或租赁给其他人使用。

EOS 网络官方声称通过使用多链并行技术,使得其目前可支持上千个商用级别的分布式应用程序正常运行。

EOS 网络在刚发布的时候采用了 DPoS 的共识机制——委托股权证明(Deligated Proof of Stake)。这种共识机制的基本原理是: 网络中的所有节点依据他们所拥有的代币的量(Stake),分配对应的投票权重;网络中的所有节点进行投票,选出一定数量的(EOS 使用的是 21 个)区块生产者进行新区块的生产与协商;区块生产者通过某种方式(随机或顺序)进行出块,且每个区块生产者通过出块来对之前的块进行确认。总的来说,由于区块生产者之间可建立直接连接从而保证通信的可靠及快速,DPoS 能在较快的时间里达成共识。

EOS 最新的白皮书中已将共识机制由 DPoS 升级为了带有拜占庭容错的委托股权证明(Byzantine Fault Tolerance – Deligated Proof of Stake),简单来说,即是将之前的“每个区块生产者通过出块来对之前的块进行确认”的机制修改为每个生产者出块后即广播该块,收到广播的区块生产者回复自己的确认消息,原区块生产者收到 2/3 以上的确认消息即将该块设置为不可逆状态。通过进行这样的修改,EOS 中区块确认时间能够进一步缩短。

EOS 的官网为 https://eos.io,其发展历程及主要大事件见图 7。

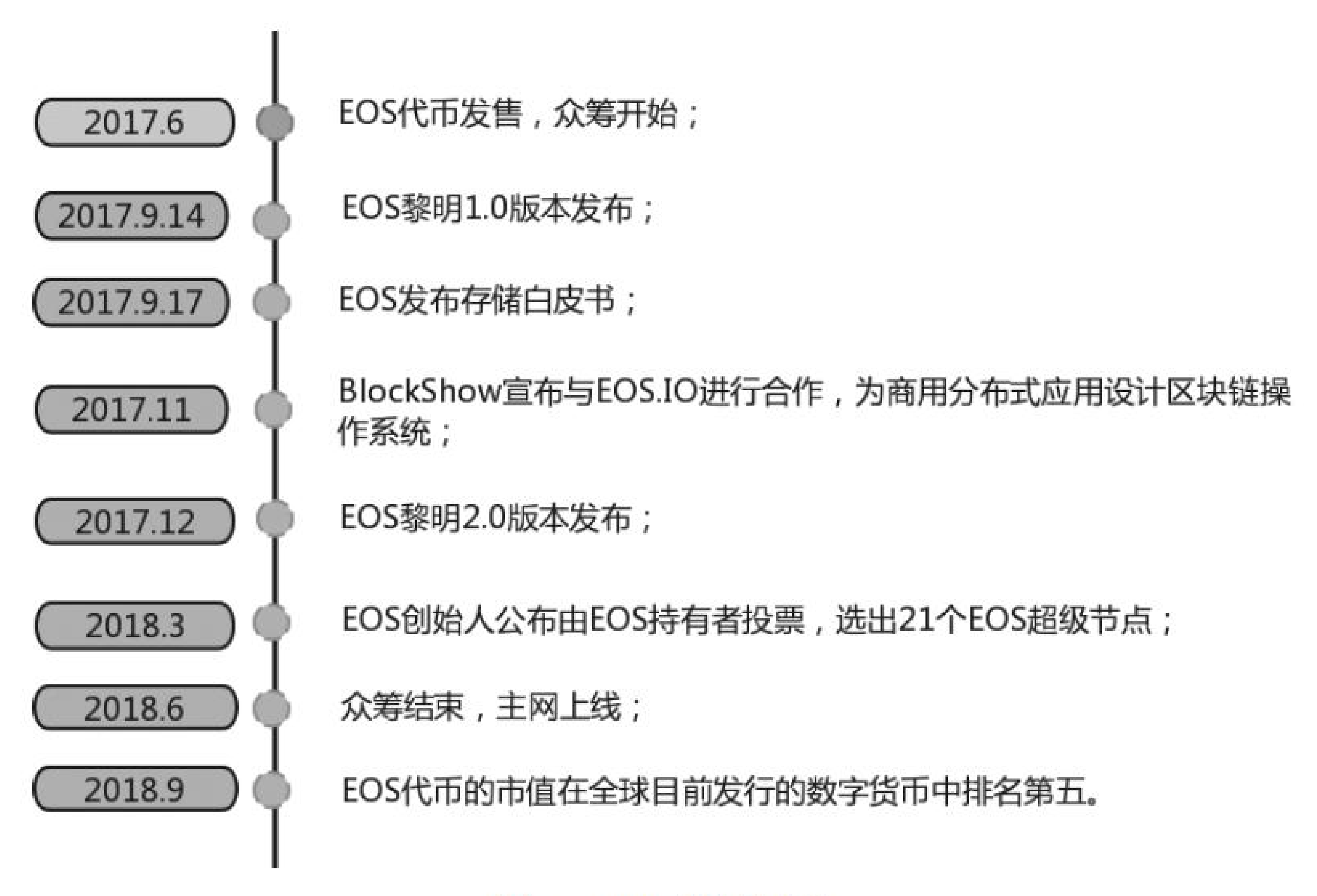


图 7　EOS 发展历程

五、瑞波网络

瑞波(Ripple)网络是一个开放的支付网络,主要用于全球范围的货币兑换及汇款。瑞波网络的提出主要是为了解决现有的集中化的国际金融交易的结算和交割所存在的缓慢、交易费昂贵的问题。依赖在瑞波网络的网关中共享的账本以及其底层的共识技术,瑞波网络能够做到即时、成本低廉的全球支付及清算,每笔交易的确认时间可以被降低至几秒的级别。

严格来说,瑞波网络并不能算是去中心化的加密数字货币。用户在交易时,需要通过瑞波网络中的瑞波网关来“代理”自己的交易。各个网关之间通过点对点通讯来对整个网络中的交易达成共识,共同维护一份交易账本。瑞波网络中的每个参与记账的节点都预先配置了一份可信任节点名单(Unique Node List,UNL),并与名单中的每个节点维护着点对点的网络连接。每间隔一段时间,瑞波网络的验证节点之间会互相交换和确认彼此的交易信息,并确认能被一定比例的验证节点承认的交易,从而达成共识。由于参与记账的节点是事先确定的,且节点间的通信很快,因此其记账效率很高,且没有 PoW 类挖矿算法的额外计算开销。当然,这也使得瑞波网络只适合于联盟链的场景。

实际上,可以将瑞波网关理解为传统意义上的银行,只是瑞波网络中的网关可以由任何可以访问瑞波网络的实体担任,包括但不限于银行、货币兑换商、交易所等。

瑞波网络理论上可以支持全球任何货币(包括各类法币以及加密数字货币)、贵金属、各类商品的交易,只需有支持这种交易的商家作为网关存在于瑞波网络之中即可。为了拓宽用户利用瑞波网络进行交易的种类及范围,瑞波网络为用户提供两种类型的交易:使用法币进行交易(xCurrent),即各银行直接通过瑞波网络进行交易;交易中使用瑞波币 XRP 作为桥梁货币(xRapid),即首先通过瑞波网关将待交易法币转换为 XRP 代币,在瑞波网络中进行 XRP 的转账,交易接收方再将代币通过对应的网关转换为法币。

由于瑞波网络在跨境支付、清算方面所表现出的优势,越来越多的银行选择开展与瑞波网络的合作。截至目前,全球 Top50 的银行集团有不少已加入了瑞波网络。上海华瑞银行于 2017 年 2 月宣布正在与瑞波联合开发跨境汇款创新产品。

需要说明的一点是,瑞波网络对应的代币 XRP 与其他大部分加密数字货币不同,并没有“挖矿”的发行机制,而是采用派送和购买的方式进行对用户的分配。这与 XRP 在瑞波网络中的作用有关,XRP 本身的价值与瑞波网络的运转是解耦的,类似于以太坊中的“燃料”,瑞波网络中的每笔交易的开展是需要消耗十万分之一 XRP 作为手续费的,且这部分 XRP 一经消耗就彻底销毁。瑞波网络希望通过这种方式防止恶意用户在其中发布大量恶意交易。从这个角度讲,由于被赋予了实际的使用价值,XRP 的价格实际上是存在潜在上限的,即“十万分之一”的 XRP 的价格是不能超过原有银行体系中境外汇款或交易的手续费的,否则用户便不会选择瑞波网络进行支付,XRP 也随之失去了作用。

瑞波网络的官网为 https://ripple.com,其发展历程及主要大事件见图 8。

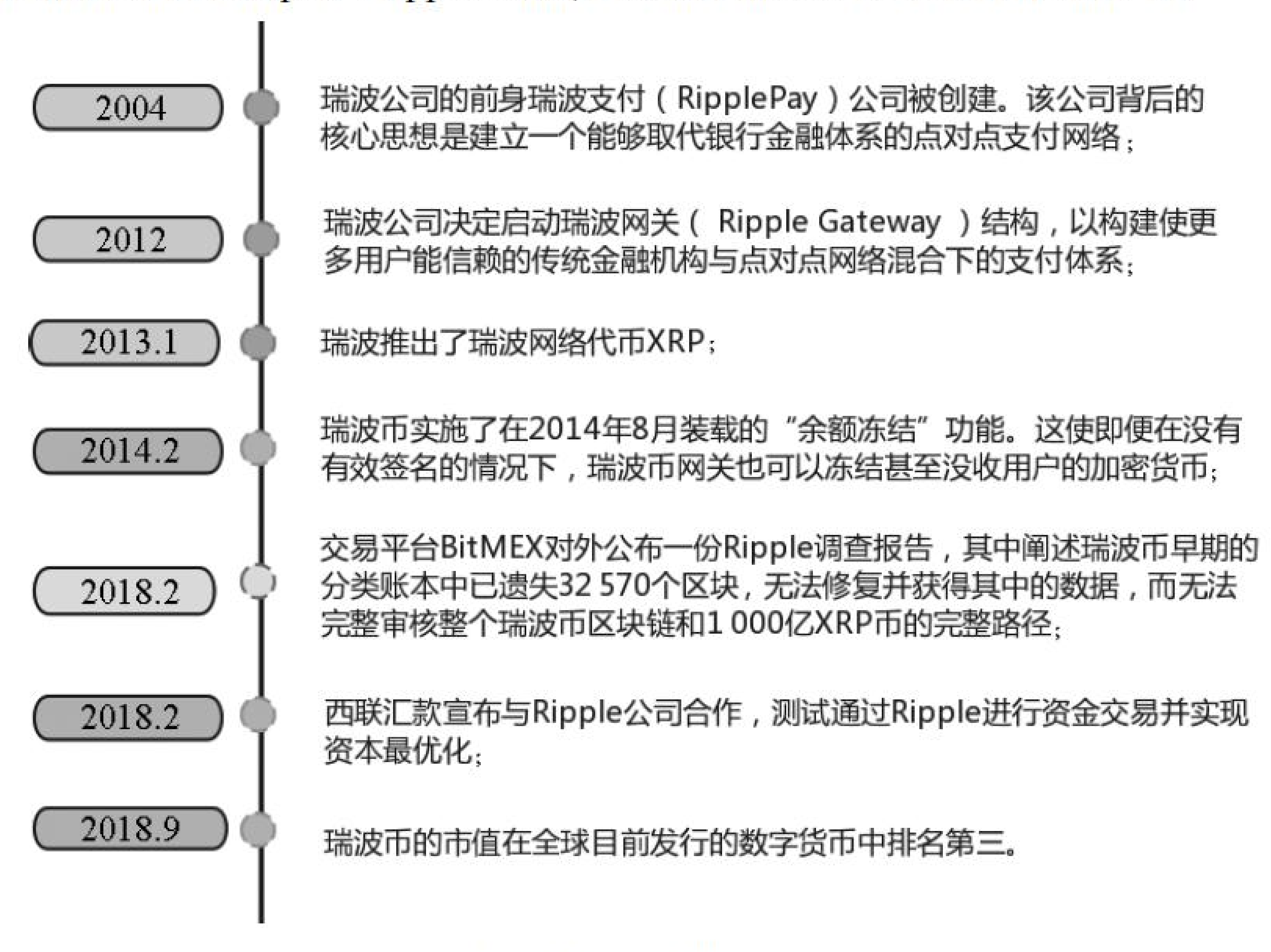


图 8　瑞波网络发展历程

六、IOTA

IOTA 是一种适用于物联网场景下的小额支付的开源分布式账本，由 David Sønstebø、Sergey Ivancheglo、Dominik Schiener 及 Dr. Serguei Popov 在 2015 年推出。IOTA 主要致力于提供物联网中各个机器之间的安全通信及付款，应用场景包括支付停车费、传感器向太阳能电网购买少量电力、支付一次扫地机器人的清扫费等。

为了适应物联网节点种类数量繁多，存在的交易种类较多、交易量大、单笔交易额度较小的特点，IOTA 采取了如下的设计思路：

（1）系统中币的数目是在创世区块就已确认的$(3^{33}-1)/2$个，总数不变，不需开采，参与节点没有挖矿的过程，从而避免了挖矿过程中不必要的能耗损失；

（2）底层选用的共识协议 Tangle 将传统区块链中的区块组织成为有向无环图（DAG），其好处在于区块间互相验证，确认交易时间快，每秒钟能够处理的交易量较大，且网络中参与共识的节点越多，交易量越大，交易的确认速度及确认度越高。

然而，IOTA 所采用的对区块 DAG 形式的组织也存在着一些问题，如交易量不足导致的区块确认度低、容易被攻击者通过生成大量交易的手段而控制等弱点。目前，IOTA 官方通过放置一个闭源的 coordinator 的方式来对上述问题进行暂时的解决。该中心化的 coordinator 定期发送 milestone 交易从而对系统中的一些交易进行确认。这在一定程度上解决了节点数目较少的时候共识容易被恶意节点群掌控的问题，然而，coordinator 的存在就有中心化的意味。如何有效地移除该中心化的 coordinator，并建立一个具有良性激励机制的去中心化 coordinator 群体，仍是 IOTA 需要解决的问题。

IOTA 的官网为 https://www.iota.org，其发展历程及主要大事件见图 9。

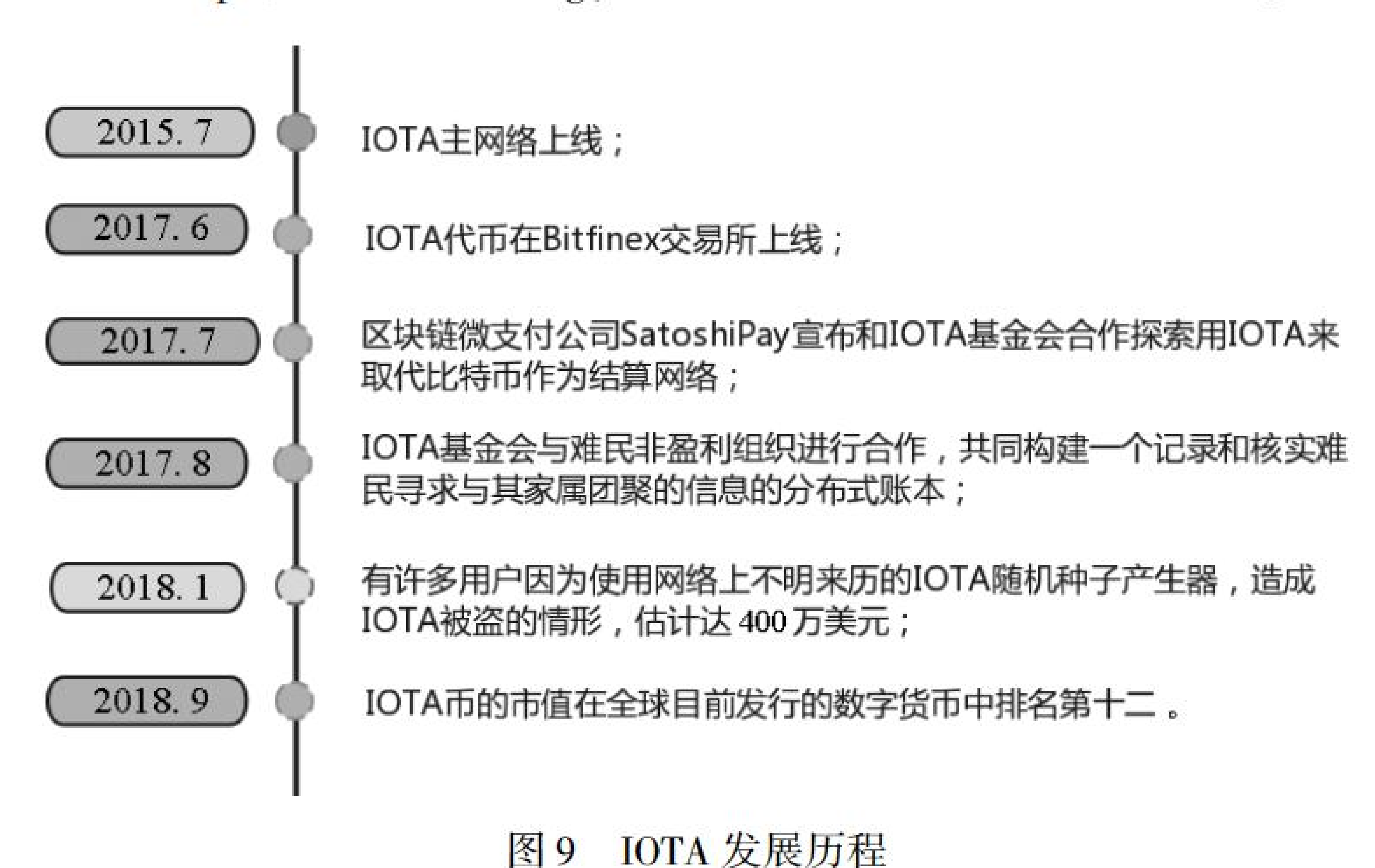


图 9　IOTA 发展历程

七、超级账本

超级账本（Hyperledger）是首个面向企业应用场景的开源分布式账本平台。该项目于

2015 年 12 月由 Linux 基金会牵头并联合 30 家初始成员（包括 IBM、Accenture、Intel、J. P. Morgan、R3、DAH、DTCC、FUJITSU、HITACHI、SWIFT、Cisco 等）宣布成立。超级账本项目首次提出和实现的完备权限管理、创新的一致性算法和可拔插的框架，对于区块链相关技术和产业的发展都将产生深远的影响。

目前，超级账本项目的主要顶级项目如下：

（1）Fabric：区块链的基础核心平台，支持可插拔的共识选择和权限管理，使用户可以根据应用场景和错误模型、通信模型自由地对平台进行配置。该项目最早由 IBM 和 DAH 发起。

（2）Sawtooth Lake：是 Intel 主导的区块链平台，利用 Intel 芯片所提供的可信执行环境的特性，支持全新的共识机制 Proof of Elapsed Time（PoET）。

（3）Iroha：主要面向 Web 和 Moblie 的账本平台项目，由 Soramitsu 发起。

（4）Blockchain Explorer：由 DTCC、IBM、Intel 等开发支持，提供一个可以快速查看绑定区块链的状态信息（如区块个数、交易历史）的 Web 操作界面。

（5）Cello：由 IBM 团队发起，提供区块链平台的部署和运行时管理功能。

（6）Indy：提供基于分布式账本技术的数字身份管理机制，由 Sovrin 基金会发起。

（7）Composer：由 IBM 团队发起并维护，提供面向链码开发的高级语言支持，自动生成链码代码等功能。

（8）Burrow：由 Monax 公司发起，提供以太坊虚拟机的支持，以实现支持高效交易的带权限的区块链平台；

Hyperledger 的官网为 https://www.hyperledger.org，其发展历程及主要大事件见图 10。

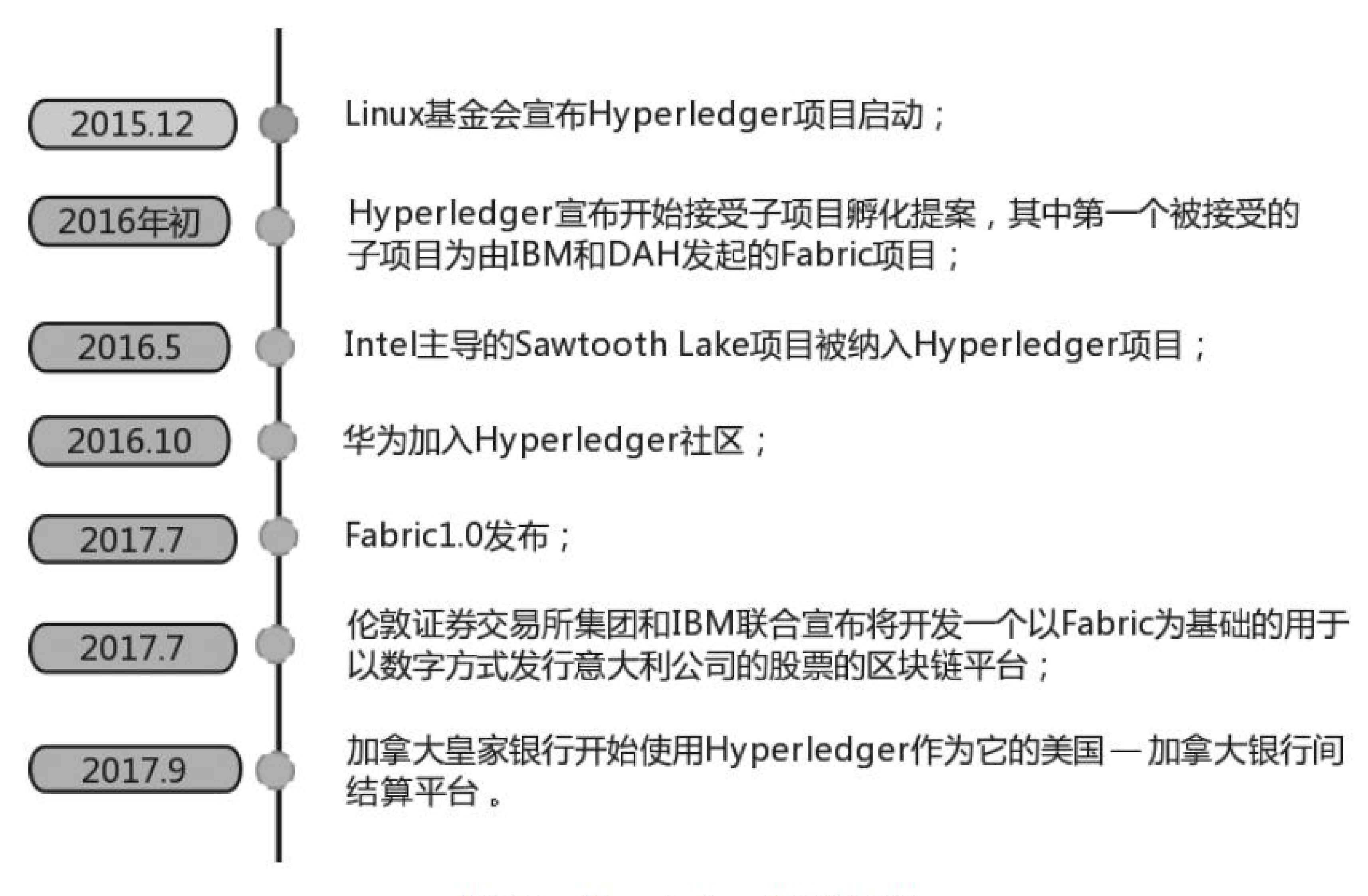


图 10　Hyperledger 发展历程